MÁSTER UNIVERSITARIO EN DERECHO DEL TRABAJO Y RELACIONES LABORALES

TRABAJO FIN DE MÁSTER

Curso académico 2019-2020

EL TRABAJADOR CHILENO EN DEMANDA DEL MODELO EUROPEO DE PROTECCIÓN DE DATOS PERSONALES

Autor: Mg. Pablo Reyes Carreño

Tutor académico: Profesor Doctor José Antonio Baz Tejedor

Salamanca Junio 2020

ÍNDICE

ABREVIATURAS

CE: Constitución Española de 1978

CDFUE: Carta de Derechos Fundamentales de la Unión Europea

ET: Estatuto de los Trabajadores

LOPDP-GDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de los Datos Personales y Garantía de los Derechos Digitales

OCDE: Organización para la Cooperación y Desarrollo Económicos

RGPD: Reglamento General de Protección de Datos de la Unión Europea 2016/679, de 27 de abril de 2016

STC: Sentencia del Tribunal Constitucional Español

TEDH: Tribunal Europeo de Derecho Humanos

"¿Qué le sucede a un amo sin esclavo?

Acaba por aterrorizarse a sí mismo.

¿Y a un esclavo sin amo?

Acaba por explotarse a sí mismo.

Hoy los dos están reunidos en la forma moderna de la servidumbre voluntaria: sujeción a los sistemas de datos, a los sistemas de cálculos; eficacia total, perfomance total.

Nos hemos convertido en dueños, por lo menos virtuales, de este mundo, pero el objeto de este dominio, la finalidad de este dominio, ha desaparecido."

Jean Baudrillard

I. INTRODUCCIÓN

Las palabras del filósofo francés Jean Baudrillard sirven para representar el momento que enfrenta el sistema de relaciones laborales a causa del cambio en el modelo capitalista de producción. La generación de riqueza con base en la depredación de recursos naturales y la apropiación de la fuerza laboral, paulatinamente ha derivado a la obtención de utilidades mediante la especulación financiera y la transacción de intangibles como el conocimiento o la información.

Si bien, dicha constatación presenta como plausible la desaparición progresiva de la estructura binominal capital-trabajo, y en consecuencia, la alteración de las relaciones jurídicas que de él derivan (entre ellas el contrato de trabajo), una dosis de apego a la realidad obliga a entender que dicho proceso tardará varias décadas en consolidar un nuevo modelo.

Sin embargo, la nueva configuración socioeconómica ya presenta algunas manifestaciones, entre ellas, la irrupción digital y las nuevas formas de trabajo, aspectos sobre los que el mundo empresarial ha comenzado a redituar.

Y no podía ser de otra forma si, entre las virtudes más rescatables del capitalismo, está su capacidad de incorporar a la comercialización todo cuanto pueda existir, incluso las huellas de interacciones que el ser humano deja mediante el uso de medios tecnológicos.

Los datos, ofrecen posibilidades de un mayor desarrollo económico mediante el uso de herramientas como big data, que pueden mejorar los procesos productivos e incluso ofrecer solución a problemas de índole social como el tratamiento de enfermedades, la administración del Estado, etc.

Empero, también son conocidos los efectos perniciosos que derivan de un aprovechamiento de la tecnología desconociendo al ser humano como destinatario de tales mejoras, por lo que debe resguardarse un ejercicio ético y respetuoso del tratamiento de datos, por ser adelantos particularmente lesivos de derechos fundamentales como la privacidad.

Europa y Latinoamérica carecen de una posición de privilegio en el uso de tecnologías como big data o inteligencia artificial, las que principalmente derivan hoy de la industrica de fabricación de dispositivos inteligentes, administración de redes sociales, y servicios de cloud o almacenamiento en la nube.

No obstante, y quizás por la baja oposición de intereses económicos directos, se ha dado curso a un desarrollo normativo en cuya formación los juristas de esta época tienen la oportunidad de aportar. Particularmente, los especialistas en el ámbito de las relaciones laborales tenemos un rol en la definición de la nueva cuestión social, y así responder al llamado contenido en el considerando 4 del Reglamento General de Protección de Datos, en virtud del cual, el tratamiento de datos personales debe estar concebido para servir a la humanidad.

En este trabajo se busca describir la evolución y fisonomía actual del sistema normativo europeo en materia de protección de datos personales, junto a su correlativa manifestación en el ordenamiento jurídico español, particularmente, en los aspectos referidos al resguardo de la privacidad de las personas físicas en el ámbito de las relaciones laborales.

Junto con lo anterior, se plantea como objetivo definir las características fundamentales del derecho de protección de datos personales a nivel europeo, a modo de

acercamiento al modelo europeo en aras de una proyección específica, con el fin de evaluar la procedencia de que tales construcciones sean utilizadas en la elaboración de reformas legales de aplicación en Chile, conforme a las singulares estructuras sociales y jurídicas de cada ámbito geográfico.

Para el desarrollo de tales objetivos resulta forzoso que, desde ya, se atienda al mandato contenido del artículo 88 del RGPD, que abre el camino hacia el derecho a la protección de datos personales de los trabajadores, en el sentido de que tales normas deberán incluir medidas adecuadas y específicas para preservar la dignidad humana, sus intereses legítimos y derechos fundamentales.

En España, la LOPDP-GDD, incorporó el artículo 20 bis al ET, significando una concreción de los derechos específicos referidos a la protección de datos personales, reservándose un desarrollo más amplio en los artículos 87 a 90 de la LOPDP-GDD.

Entonces, se trataría de un primer núcleo básico de derechos digitales ejercitables en el ámbito laboral, con la vista puesta en otorgar claridad respecto de ciertas situaciones de evidente conflictividad y de disparidad en la aplicación de los criterios de ponderación.[1]

A juicio de la comunidad jurídica, quedarían pendientes otros aspectos relevantes y de creciente conflictividad, como son: el uso de sistemas biométricos de identificación, o el uso de inteligencia artificial para la evaluación de expedientes laborales y su eventual uso para decisiones automatizadas que involucren una valoración de los trabajadores. [2]

En Chile, la normativa sobre protección de datos personales está en vigor desde 1999, y sus modificaciones no han incorporado aspectos centrales en comparación con el modelo europeo o las recomendaciones de la OCDE.

Entre los aspectos que urge atender, existen brechas tanto desde el punto de vista sustantivo como procedimental. Se reclama la existencia de un catálogo más amplio de derechos de los interesados y una conducta de mayor responsabilidad por parte de quien ejecuta el tratamiento de datos.

A nivel constitucional, el derecho a la protección de datos personales se incorporó al conjunto de derechos fundamentales en 2018, y la jurisprudencia no ha dado signos de una interpretación que satisfaga las circunstancias actuales de alta digitalización.

Actualmente, está en tramitación un proyecto de ley que moderniza la legislación en materia de protección de datos, pero su tramitación se ha visto retrasada por las circunstancias políticas derivadas primeramente del movimiento social iniciado en octubre de 2019, y más recientemente, la crisis derivada de la pandemia de Covid-19.

También se analizará el rol que ha cumplido la Dirección del Trabajo de Chile, institución que, conforme a sus fines institucionales, está facultada para interpretar la legislación laboral.

La actuación del servicio de inspección en lo laboral, a falta de otra autoridad competente, resulta de interés para comprender el sentido otorgado a las escasas y

---

[1] BAZ RODRÍGUEZ, J., "La ley orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales,* Nº 54, 2019, págs. 49-78.

[2] GOÑI SEIN, J.L., "Uso de los dispositivos digitales en el ámbito laboral", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Monográfico Nº 11, 2020.

limitadas disposiciones que sobre protección de datos contempla el Código del Trabajo chileno.

Conforme a tales objetivos y la estructura adoptada para su desarrollo, se ha optado por omitir el análisis pormenorizado de las situaciones fácticas ya resueltas por la jurisprudencia española o del TEDH. Sin embargo, se ha incorporado la revisión de la plataforma Teams de Microsoft desde la perspectiva de la normativa de protección de datos, con el fin de ejemplificar la urgente necesidad de debate en torno a las herramientas tecnológicas puestas a disposición de los trabajadores.

Con todo, se espera contribuir –desde la perspectiva ius laboralista– al debate destinado a estructurar el nuevo régimen de protección de datos personales en Chile, bajo un sentido de reflexión y compromiso con el mundo del trabajo inculcado por la Escuela Salmantina durante mi valorada etapa de formación en el Máster en Derecho del Trabajo y Relaciones Laborales.

II. PROTECCIÓN DE DATOS PERSONALES: FISONOMÍA DE UN MODELO

A. Privacidad y Protección de Datos: Luego de un siglo, algunas ideas claras

La privacidad es un concepto de difícil articulación semántica, y actualmente puede abarcar: libertad de pensamiento, control sobre el cuerpo, control sobre la información personal, libertad de vigilancia, protección de la reputación y contra búsquedas e interrogatorios. [3]

La amplitud y evanescencia del concepto ha llevado a confusión, acrecentada por las diversas acepciones que se observan según sean los sistemas jurídicos en que se analice.

De esta forma, si bien la Constitución de los Estados Unidos no contiene explícitamente la palabra *Privacy*, la Corte Suprema ha entendido que la cuarta enmienda protege contra intromisiones del gobierno cuando la persona tiene una expectativa razonable de privacidad.

Dicho estatus de reconocimiento a la privacidad, deriva de los primeros casos analizados a finales del siglo XIX, especialmente en el artículo Warren & Brandeis *The Right to Privacy*, publicado en la Revista de la Universidad de Harvard en 1890.

En dicho artículo, se esboza la existencia de un *The Right to be let alone*, entendido como el derecho a ser dejado en paz, idea fundacional de la privacidad para américa y europa.

Sin embargo, el concepto de protección de datos como elemento autónomo de la privacidad, se reconoce como una creación jurídica propia de Europa, donde además se le otorga el carácter de derecho fundamental diferenciado. [4]

Dicha fisonomía particular, se advierte a nivel jurisprudencial en la sentencia del Tribunal Constitucional Alemán sobre la Ley del Censo de 1983, oportunidad en que se reflexiona sobre el derecho a la autodeterminación informativa, del que luego derivaría el derecho a la protección de datos, todo en el marco de sociedades cada vez más tecnologizadas, en las que la ausencia de control sobre el manejo de la información podría implicar un impedimento en las posibilidades de desarrollo para el individuo.

En el ámbito de la legislación interna de los países europeos, se señalan como hitos de la caracterización diferenciada de la protección de datos frente a la privacidad, la Ley de Protección de Datos del Estado de Hesse de septiembre de 1970, Ley sueca de Protección de Datos (1973), y la Ley francesa sobre informática y ficheros y libertades individuales (1978). [5]

A nivel supranacional, surgen instrumentos internacionales primeramente influenciados por la teoría norteamericana, vinculándose a principios de los años 80 a la

---

[3] SOLOVE, D., "Understanding Privacy", *GWU Legal Studies Research Paper*, Nº 420, 2008. Disponible en https://ssrn.com/abstract=1127888

[4] PÉREZ MIRAS, J., *El Derecho a la Protección de Datos y a la Privacidad. Una perspectiva comparada entre la Unión Europea y Estados Unidos,* Tesis Doctoral, Universidad de Sevilla, 2018. Disponible en https://idus.us.es/handle/11441/83475

[5] KUNER, C., "An international legal framework for data protection: Issues and prospects", *Computer Law & Security Review,* Vol. 25, 2009, págs. 307-317. Disponible en https://doi.org/10.1016/j.clsr.2009.05.001

preservación de la privacidad. Así se observa en las Directrices de la OCDE de 1980, y sobretodo, en el primer instrumento internacional sobre la materia jurídicamente vinculante: Convenio 108 del Consejo de Europa, de 1981.

Justamente, el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, de 28 de enero de 1981, y ratificado por España el 27 de enero de 1984, determinó la estructura básica de la normativa sobre protección de datos personales actualmente vigente en europa.

Ambos instrumentos reseñados (Directrices de la OCDE y Convenio 108 del Consejo de Europa), tienen el propósito de eliminar barreras a la libre circulación de datos, con el particular interés de salvaguardar las incipientes actividades económicas, que vislumbraban en la información un importante insumo productivo.

Sin perjuicio de aquello, el Convenio 108, incorporó garantías que fueron recogidas en la Directiva 95/46/CE [6]: Principio de calidad de los datos, limitación según el propósito del tratamiento, procesamiento leal y lícito, tratamiento para fines específicos y legítimos, etc. [7]

En el mismo sentido, el artículo 6 consagra las categorías particulares de datos, considerando por tales, aquellas que revelan el origen racial, las opiniones políticas, convicciones religiosas u otras, así como datos personales relativos a la salud o a la vida sexual; imponiéndose como primera medida de protección la prohibición de las gestión automatizada de dichos datos. [8]

A pesar de lo anterior, la definición de objetivos del Convenio 108 fija su campo de acción en el respeto a la vida privada frente al tratamiento automatizado de los datos personales, circunstancia que mutará con la redacción del artículo 8 de la CDFUE. [9]

En efecto, el artículo 8 de la CDFUE contempla específicamente el derecho a la Protección de Datos de carácter personal, al preceptuar que:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.

---

[6] Directiva 95/46/CE, del Parlamento Europeo y el Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[7] Baz Rodríguez, J., *Privacidad y protección de datos de los trabajadores en el entorno digital*, Ed. Wolters Kluwer, Madrid, 2019, pag. 57.

[8] En aspectos centrales, como el concepto de dato personal o el contenido de las categorías especiales de datos personales, la legislación vigente en Chile mantiene el contenido normativo descrito en el Convenio 108.

[9] La CDFUE fue proclamada por el Parlamento Europeo, la Comisión Europea y el Consejo de la UE en diciembre de 2000. Con la entrada en vigor del Tratado de Lisboa el 1 de diciembre de 2009, la CDFUE pasó a ser un instrumento jurídicamente vinculante para España, aplicándose según lo dispone el artículo 10.2 de CE, norma que impone un sentido de interpretación de las libertades y derechos fundamentales en conformidad a la Declaración Universal de Derechos Humanos y los Tratados ratificados por España.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente. [10]

De esta forma, por primera vez en la UE se consagra la protección de datos como derecho fundamental de naturaleza autónoma, y se establecen algunas garantías específicas, a saber: que los datos personales deben procesarse de manera justa para fines específicos y sobre la base del consentimiento de la persona interesada o sobre alguna otra base legítima establecida por la ley, que existe un derecho de acceso y de rectificación a los datos recopilados, y que el cumplimiento de estas reglas estará sujeto al control de una autoridad independiente. [11]

Finalmente, sobre tales bases se aprobaría el RGPD, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por el que además se deroga la Directiva 95/46/CE.

Se constituye así un verdadero derecho fundamental de raíz comunitaria, consistente en que *"toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan",* bajo el principio tutelar de que el RGPD "*protege los derechos y libertades fundamentales de las personas físicas, y en particular, su derecho a la protección de datos personales"*. [12]

Por todo lo anterior, el RGPD ha supuesto un cambio de paradigma en el modelo europeo de protección de datos, que ha derivado en la necesidad de adaptar la normativa interna por dos razones: [13]

- Como reforzamiento de la seguridad jurídica mediante una depuración de la normativa interna, y

- Para el desarrollo de la normativa comunitaria en aquellas aspectos en que aquella lo precisa o lo prevé.

Junto con ello, el reglamento pone de relevancia la protección de datos en el ámbito laboral, al considerar explícitamente dicho contexto de relaciones humanas, lo que resulta de especial relevancia conforme a las particulares vinculaciones que se generan en el ámbito de las relaciones de trabajo.

Dicho cambio de paradigma también se advierte en la concepción de un principio de privacidad desde el diseño, por el que la privacidad se erige como un valor que debe incorporarse de forma transversal en toda organización, de manera que resulte posible anticiparse a cualquier atentado o desviación de su contenido. Así, la empresa debe estar en condiciones de proteger de forma automática la privacidad, como resultado de una

---

[10] Según las explicaciones a este artículo elaboradas bajo la responsabilidad del Praesidium de la Convención que redactó la la Carta, la actual redacción se basó en el artículo 286 del Tratado constitutivo de la Comunidad Europea (sustituido por el artículo 16 del Tratado de Funcionamiento de la UE y el artículo 39 del Tratado de la UE) y en la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981.

[11] MARTÍNEZ LÓPEZ-SÁEZ, M., "La vigilancia electrónica en el contexto laboral europeo y estadounidense: perfilando el derecho a la protección de datos en el trabajo", *Revista General de Derecho del Trabajo y de la Seguridad Social,* Nº 47, 2017.

[12] BAZ RODRÍGUEZ, J., *Privacidad y protección… Op. Cit*. pag. 58.

[13] BAZ RODRÍGUEZ, J., "La ley orgánica 3/2018…" *Op. Cit.*

estructura técnica y organizativa de protección "por defecto" asimilada en todas las esferas del negocio. [14]

B. La Protección de Datos Personales como derecho autónomo en la jurisprudencia española

Atendida la circunstancia de que el actual modelo europeo de protección de datos –primeramente con la CDFUE y luego con la entrada en vigor del RGPD– efectúa una separación material entre la privacidad y el derecho de protección de datos personales, cabe analizar si dicha división de cauces ha ocasionado consecuencias prácticas o jurídicas de cierta entidad.

A este propósito, resulta útil revisar el criterio de los tribunales superiores de justicia, en particular, respecto a la manera en que han recogido y aplicado la protección de datos como derecho fundamental autónomo.

Sobre este punto, el Tribunal Constitucional Español, a falta de una mención expresa a nivel de la Carta Fundamental, ha procurado fijar los elementos diferenciadores entre la intimidad y la protección de datos.

Tal ejercicio de desarrollo doctrinal, ha pasado por tres momentos fundamentales:

1. La protección de datos como garantía de intimidad.

En esta etapa, la jurisprudencia del Tribunal Constitucional se manifiesta en el sentido de que la implantación de los medios tecnológicos podría derivar en su uso abusivo, respecto del que que se desconocía su alcance, pero que sin lugar a dudas sería atentatorio del derecho a la intimidad.

Bajo la lógica jurídica imperante, no se concebía un uso abusivo de los medios informáticos sin que previamente se constatara un atentado a la intimidad, razón por la que el debate judicial se centraba en el artículo 18.1 CE, en tanto que, el artículo 18.4 CE tenía una aplicación de carácter residual, y por tanto, escasamente invocado.

A esta etapa corresponde la STC 142/1993, de 22 de abril, en la que se discute si cierto precepto legal sería inconstitucional por atentar en contra del derecho a la intimidad personal reconocido en el artículo 18.1 CE, toda vez que, impone la obligación a los empresarios de entregar a los representantes de los trabajadores una copia básica de los contratos que deban celebrarse por escrito.

Entonces, el tribunal se centra en dilucidar la eventual afectación del derecho a la intimidad, en particular, respecto a los datos económicos de las personas, resolviendo en favor del rol que le corresponde a los representantes sindicales, referido a velar por el cumplimiento de la legislación laboral, razonando en los siguientes términos:

"Del mismo modo que los representantes legales pueden llegar a tener competencias de vigilancia y control del correcto cumplimiento de la legislación laboral, no cabe duda que las organizaciones sindicales tienen un interés directo en el mismo que, sin duda, se encuentra recogido entre los "económicos y sociales que les son propios" cuya defensa les encomienda la Constitución (art. 7").[15]

Entre otros argumentos esgrimidos por los tribunales destacan aquellos expresados en la STC 110/1984, de 26 de noviembre, que en procedimiento de amparo

[14] BAZ RODRÍGUEZ, J., *Privacidad y protección… Op. Cit*. pag. 81.

[15] FJ 10, STC 142/1993, de 22 de abril.

desestimó acoger la concurrencia de una vulneración del derecho a la intimidad personal y familiar de un contribuyente acusado de fraude al fisco, a quien mediante resolución administrativa se le exige aportar antecedentes referidos a sus movimientos crediticios.

La particularidad de este temprano pronunciamiento, más que en el carácter desestimatorio de la acción constitucional, el interés recae en la argumentación referida a la amplitud y adaptación que ha debido sufrir –en cuanto a su contenido– el derecho a la intimidad personal, particularmente al expresar que:

"El reconocimiento explícito en un texto constitucional del derecho a la intimidad es muy reciente y se encuentra en muy pocas Constituciones, entre ellas la española. Pero su idea originaria, que es el respeto a la vida privada, aparece ya en algunas de las libertades tradicionales. La inviolabilidad de domicilio y de la correspondencia, que son algunas de esas libertades tradicionales, tienen como finalidad principal el respeto a un ámbito de vida privada personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado. Lo ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida. No siempre es fácil, sin embargo, acotar con nitidez el contenido de la intimidad". [16]

Entonces, se advierte como particularidad de esta etapa de la doctrina judicial una aproximación frente a los usos abusivos de los datos personales, enmarcada en la garantía de la intimidad personal, mirándose el uso de los medios informáticos como situación de particular riesgo o amenaza de aquel derecho.

2. La protección de datos y la privacidad: dos caras de la misma moneda.

Un segundo momento jurisprudencial logra caracterizar al derecho a la protección de datos personales, empero, sin alcanzar la categoría de derecho fundamental autónomo.

Así, la STC 254/1993, de 20 de julio, es clara al advertir que *"el uso de la informática encuentra un límite en el respeto al honor y la intimidad de la personas y en el pleno ejercicio de sus derechos. Ahora bien, la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España. Pues, como señala el Ministerio Fiscal, la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)"*.

En este momento temprano de la conceptualización judicial del derecho a la protección de los datos personales, el Tribunal Constitucional entiende que aquél corresponde a la faz positiva del derecho a la intimidad personal, por lo que el

[16] FJ 3, STC 110/1984, de 26 de noviembre.

desconocimiento de las facultades de control sobre los datos personales deriva en impracticable el ejercicio del derecho a la intimidad. [17]

También es cierto que el desarrollo tecnológico evidenció un importante incremento durante la década de 1990 (internet, ofimática, bases de datos, etc.), lo que tuvo por efecto delinear una nueva realidad social, que forzó a la elaboración de nuevas construcciones jurídicas, mismas que, a nivel jurisprudencial, implicaron reconocer al ciudadano ciertas facultades de control sobre sus datos personales.

En este contexto, la acción de amparo deducida por un trabajador en contra del empresario que creó un fichero automatizado sobre absentismos laborales por baja producida por enfermedad común o accidente laboral, resulta acogida, entendiéndose la medida como vulneratoria del derecho a la intimidad personal contenido en el artículo 18.1 de la CE, sin perjuicio de que los argumentos fundantes acusan infracciones a las normas sobre tratamiento de datos personales, por ejemplo: no registrar el fichero ante la autoridad protectora de datos, no acceder a la cancelación de los datos, etc.

Bajo una lógica propia de esta etapa de la jurisprudencia, el tribunal en este caso razona bajo el carácter garantista que reviste la libertad informática, al expresar:

"...la garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona; la llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención (SSTC 254/1993, fundamento jurídico 7º; 11/1998, fundamento jurídico 4º; 11/1998, fundamento jurídico 4º y 94/1998, fundamento jurídico 4º)". [18]

Y en definitiva se acoge el amparo deducido, por infracción a la intimidad del recurrente.

3. La protección de datos personales como derecho fundamental autónomo.

Dan cuenta de este período dos sentencia fundamentales, STC 290/2000 y STC 292/2000, ambas de 30 de noviembre; pronunciamientos judiciales emitidos bajo el contexto de la recien estrenada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La primera de las sentencias, describe las funciones concedidas por la ley a la Agencia de Protección de Datos, las que define como de carácter público y esencialmente preventivas de la protección de datos personales. Pero el aporte principal del fallo, radica en concebir la protección de datos como derecho autónomo, al manifestar:

"...el derecho fundamental al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos

[17] FJ 8, STC 254/1993, de 20 de julio.

[18] FJ 2, STC 202/1999, de 8 de noviembre.

personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos".

"En suma, el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos. De suerte que es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes". [19]

Por su parte, la STC 292/2000, de 30 de noviembre, consolidó el carácter de derecho autónomo de la protección de datos, al precisar que:

"...el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo".

"Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido…". [20]

"...el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos

[19] FJ 7, STC 290/2000, de 30 de noviembre.

[20] FJ 6, STC 292/2000, de 30 de noviembre.

datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos". [21]

Con todo, el contexto jurídico en que fueron emitidas estas sentencias favoreció a que el derecho a la protección de datos personales fuera reconocido con carácter de derecho fundamental autónomo, y no solo como garantía para el ejercicio de otros derechos. Con este nuevo enfoque se habilita para el ejercicio directo ante los tribunales y órganos administrativos, en procura de resguardar su contenido, concebido más ampliamente que la forma en que el constituyente los inscribió en el artículo 18.4 CE.

Como se analizará, además la STC 292/2000 incide directamente en el modelo constitucional chileno, puesto que durante la discusión parlamentaria fue reiteradamente invocada como referente a la hora de concebir la protección de datos como derecho autónomo.

C. La jurisprudencia Chilena: Reconocimiento de un derecho para su destrucción

En Chile, el derecho a la protección de datos se incorporó a la Constitución Política de la República mediante la promulgación de la Ley Nº 21.096 publicada en el Diario Oficial el 16 de junio de 2018. [22]

Dicha reforma constitucional fijó la redacción del artículo 19 Nº 4 de la carta fundamental en los siguientes términos:

"Artículo 19.- La Constitución asegura a todas las personas:"

"Nº 4.- El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley;"

Del tenor literal se advierte una clara diferenciación entre la protección de la vida privada y la honra, frente a la protección de datos personales.

A mayor abundamiento, la adopción de un modelo de protección de datos como derecho fundamental autónomo, queda en evidencia durante la tramitación del proyecto de ley de reforma constitucional. Según da cuenta la historia de la ley, en la presentación del proyecto –iniciado por moción parlamentaria– se propone que:

"Siguiendo a lo expresado por la magistratura constitucional española, es necesario consagrar en nuestro país el derecho a la protección de datos como un derecho autónomo, independiente, y con un contenido diferente del derecho a la protección de la vida privada, que merece ser reconocido y protegido por el ordenamiento jurídico. Sin perjuicio de lo anterior, la presente reforma propone su regulación en el artículo 19 n° 4 de la CPR, ya que reconoce que se trata de un derecho derivado de la intimidad, y es en ese entendido, la razón de su ubicación".

Se destaca como característica del modelo constitucional que se pretende adoptar, aquel descrito por el Tribunal Constitucional Español en STC 292/2000, de 30 de noviembre, pronunciamiento judicial que según hemos informado en párrafos que

---

[21] FJ 7, STC 292/2000, de 30 de noviembre.

[22] BIBLIOTECA DEL CONGRESO NACIONAL, *Historia de la Ley Nº 21.096, de 16 de junio de 2018.* Disponible en: https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/7551/

anteceden, marca la etapa del reconocimiento a la protección de datos como derecho autónomo en el ámbito judicial español.

Luego, avanzada la tramitación, el Senador Harboe (uno de los parlamentarios que presentaron la moción), manifestó durante la discusión en sala que:

"En el Tribunal Constitucional chileno ha habido una evolución jurisprudencial en el sentido de reconocer que los datos personales constituyen un derecho de los ciudadanos, y más aún, que son un derecho de tercera generación, autónomo e independiente del grado de intimidad".

"...este proyecto de reforma constitucional busca consagrar el derecho de todos los ciudadanos a la protección de sus datos personales, otorgándoles el derecho de acceso, cancelación y rectificación de aquellos datos erróneos o cuya difusión o almacenamiento genere una afectación de otros derechos".

"De igual modo, al quedar incorporado en el numeral 4° del artículo 19, se hace aplicable el recurso de protección, como una medida para restablecer el imperio del derecho, a fin de que frente a las vulneraciones de parte del mundo privado exista una herramienta constitucional para proteger este nuevo derecho". [23]

Cabe tener presente que antes de la reforma constitucional, se distinguieron dos períodos relevantes: [24]

- La protección de datos personales no se considera un problema constitucional. En este período, no obstante que el tribunal conoce situaciones que hoy claramente se identifican como relativas a la protección de datos personales, fueron resueltas bajo el criterio de evitar la lesión de la privacidad o intimidad, ambos conceptos estimados como sinónimos. [25]

- Se asume la protección de datos como problema de ámbito constitucional. Corresponden a esta etapa las sentencias roles acumulados Nº 1732-10 y 1800-10, de fecha 21 de junio de 2011, mediante las cuales el Tribunal Constitucional reconoce por primera vez que la vida privada *"asegura a todas las personas el amparo de la injerencia de terceras personas, procurando así el pleno ejercicio de la libertad personal sin interferencias ni intromisiones o presiones indebidas" y que "la protección de la vida privada de las personas guarda una estrecha relación con la protección de los datos personales, configurando lo que la doctrina llama derecho a la autodeterminación informativa"*.

Sin embargo, tal sentido evolutivo expresado en la actuación del Tribunal Constitucional chileno, y que implica el reconocimiento expreso de la protección de datos personales como derecho fundamental autónomo, no derivó en la existencia de una jurisprudencia uniforme ni consolidada, tal y como queda demostrado con la sentencia de la Corte Suprema Rol Nº 54-2020, de 10 de junio de 2020, al expresar que:

---

[23] Sesión de Senado de 03 de marzo de 2015, Sesión 94, Legislatura 362. Discusión y aprobación en particular.

[24] QUEZADA RODRÍGUEZ, F., "La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile", *Revista Chilena de Derecho y Tecnología,* Vol 1, Nº 1, Santiago de Chile, 2012, págs. 125-147.

[25] Corresponden a este período las siguientes sentencias del Tribunal Constitucional chileno: 198/94, de 4 de enero de 1995; 389/03, de 28 de octubre de 2003; 521/06, de 01 de agosto de 2006; 1365/09, de 08 de abril de 2010; y, 1683/10, de 04 de enero de 2011.

"…el llamado "derecho al olvido" no se encuentra establecido en nuestra legislación, y que los motores de búsqueda de Internet no son responsables de los datos que crean los usuarios, sino que su función se limita a indexar la información, la que es creada por terceros al amparo de la libertad de emitir opinión y de información garantizada en el artículo 19 N° 12 de la Carta Fundamental, con las limitaciones y responsabilidades allí establecidas".

Cabe expresar que, no obstante la falta de legislación específica que regule el "derecho al olvido", el máximo tribunal debió analizar la amplitud y el carácter garantista que representa el derecho a la protección de datos personales, reconocido constitucionalmente a partir del año 2018. Por el contrario, se restó de dicho razonamiento en virtud los argumentos contenidos en una sentencia anterior del mismo tribunal Rol Nº 19.134-2018, de 22 de enero de 2019, en la que se decidió:

"…resulta de interés destacar que la Ley Nº 21.096, publicada en el Diario Oficial con fecha 16 de junio de 2018, reformó el artículo 19 Nº 4 de la Constitución Política de la República, incorporando la siguiente frase: "y, asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley". De esta modificación se desprende que, sin perjuicio del explícito reconocimiento del constituyente, en lo sustancial no ha cambiado el escenario en lo que se refiere al respeto y protección del derecho a la vida privada y a la honra de la persona y su familia, pues la cautela jurisdiccional sigue estando confiada al legislador, mediante el reenvío a las disposiciones contenidas en la citada Ley Nº 19.628".

En síntesis, el sentido de la actual jurisprudencia de Corte Suprema consiste en estimar de que en Chile no obstante haberse reconocido el derecho a la protección de datos personales con rango constitucional, tal derecho solo tendrá el contenido que específicamente determine el legislador. Luego, considerando que la normativa vigente data de 1999, que no desarrolla derechos digitales conforme al actual alcance del RGPD, no contempla una autoridad competente en protección de datos, ni una acción de reclamación específica, en los hechos, el contenido constitucional se ha transformado en letra muerta.

D. El Derecho a la Protección de Datos Personales en el Trabajo: En el rol de Winston Smith 8 horas diarias

Según se ha analizado, la evolución del contenido del derecho a la protección de datos personales, permite hoy definir aquel como un un derecho fundamental autónomo, mismo que a la luz de la reiterada jurisprudencia, consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. [26]

El contexto de la relación laboral, no constituye una excepción al ejercicio de este derecho, pues como expresamente lo ha indicado el Tribunal Constitucional Español en diversas sentencias[27], el ámbito de la relación laboral no puede implicar la privación de

[26] STC 292/2000, de 30 de noviembre.

[27] Entre otras STC 88/1985, de 19 de julio; STC 126/1990, de 5 de julio; y STC 90/1997, de 6 de mayo.

los derechos fundamentales de los trabajadores, pues éstos tienen eficiacia directa e inmediata; en síntensis, la condición de trabajador no altera los derechos que la Constitución reconoce al ciudadano. [28]

En el ámbito de la jurisprudencia europea, un aporte trascendental lo constituye la sentencia del TEDH de 5 de septiembre de 2017, asunto Barbulescu contra Rumanía, conocida como Barbulescu II, es particularmente interesante pues analiza la protección que debe otorgar el sistema jurídico al tratamiento de datos sensibles en el ámbito laboral[29], efectuándose un meticuloso papel de delimitación de las fronteras de expansión del poder de control empresarial sobre las comunicaciones electrónicas del trabajador emanadas de la empresa. [30]

La sentencia antes referida, a pesar de estimar vulnerado el derecho a la intimidad y al secreto de las comunicaciones, se conecta en su razonamiento con los principios de la protección de datos al enunciar las reglas que deben dirigir toda medida empresarial de monitorización de las comunicaciones del trabajador, que a trazo grueso son: la información previa sobre la posible supervisión, la limitación de la medida de control, la concurrencia de un motivo legítimo, la estricta necesidad de monitorización, proporcionalidad y compatibilidad con el fin declarado, y garantías de lealtad en la realización de la medida.

Sin embargo, a pesar de la evolución en su contenido jurídico y social que ha exhibido el derecho a la protección de datos personales, su ejercicio por parte de los trabajadores sigue resultando de mayor sacrificio y costo, esto a causa del poder que ostenta el empleador, fundamentado en su capacidad de organización de la empresa.

Por tal razón, se ha llegado a establecer que las facultades de organización y dirección que recaen en el empresario admiten limitaciones cuando se sitúan en confrontación con los derechos fundamentales del trabajador. De allí que la STC 98/2000, de 10 de abril, dispuso que el poder de dirección del empleador resulta justificado y legítimo solo cuando satisface los objetivos que se describen en el fundamento jurídico 7:

"*En definitiva, los equilibrios y limitaciones recíprocos que se derivan para ambas partes del contrato de trabajo suponen, por lo que ahora interesa, que también las facultades organizativas empresariales se encuentran limitadas por los derechos fundamentales del trabajador, quedando obligado el empleador a respetar aquéllos (STC 292/1993, de 18 de octubre, FJ 4). Este Tribunal viene manteniendo que, desde la prevalencia de tales derechos, su limitación por parte de las facultades empresariales sólo puede derivar bien del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho (SSTC 99/1994, FJ 7, y 106/1996, FJ 4), bien de una acreditada necesidad o interés empresarial, sin que sea suficiente su mera invocación para sacrificar el derecho fundamental del trabajador (SSTC 99/1994, FJ 7, 6/1995, FJ*

[28] ÁLVAREZ CORTÉS, J.C., "La protección de datos de carácter personal en el ámbito de la relación laboral como derecho fundamental inespecífico", Monereo Pérez J.C., y otros (Dir.), *Derechos Laborales Fundamentales Inespecíficos,* Editorial Comares, Granada, 2020, pag. 326.

[29] MARTÍNEZ LÓPEZ-SÁEZ, M., "La vigilancia electrónica…" *Op. Cit.*

[30] GOÑI SEIN, J.L., "La protección de las comunicaciones electrónicas del trabajador: la doctrina del Tribunal de Estrasburgo y la jurisprudencia constitucional", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Nº 40, 2018, págs. 12-26.

3 y 136/1996, FJ 7). Pero, además de ello, la jurisprudencia constitucional ha mantenido, como no podía ser de otro modo, que el ejercicio de las facultades organizativas y disciplinarias del empleador no puede servir en ningún caso a la producción de resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador (así, entre otras, SSTC 94/1984, de 16 de octubre, 108/1989, de 8 de junio, 171/1989, de 19 de octubre, 123/1992, de 28 de septiembre, 134/1994, de 9 de mayo, y 173/1994, de 7 de junio), ni a la sanción del ejercicio legítimo de tales derechos por parte de aquél (STC 11/1981, de 8 de abril, FJ 22)".

"Por eso, este Tribunal ha puesto de relieve la necesidad de que las resoluciones judiciales, en casos como el presente, preserven "el necesario equilibrio entre las obligaciones dimanantes del contrato para el trabajador y el ámbito -modulado por el contrato, pero en todo caso subsistente- de su libertad constitucional" (STC 6/1988, de 21 de enero). Pues dada la posición preeminente de los derechos fundamentales en nuestro ordenamiento, esa modulación sólo se producirá "en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva" (STC 99/1994). Lo que entraña la necesidad de proceder a una ponderación adecuada (SSTC 20/1990, de 15 de febrero, 171/1990, de 12 de noviembre, y 240/1992, de 21 de diciembre, entre otras muchas), que respete la correcta definición y valoración constitucional del derecho fundamental en juego y de las obligaciones laborales que pueden modularlo (SSTC 170/1987, de 30 de octubre, 4/1996, de 16 de enero, 106/1996, 186/1996, de 25 de noviembre, y 1/1998, de 12 de enero, entre otras muchas)".

"Estas limitaciones o modulaciones tienen que ser las indispensables y estrictamente necesarias para satisfacer un interés empresarial merecedor de tutela y protección, de manera que si existen otras posibilidades de satisfacer dicho interés menos agresivas y afectantes del derecho en cuestión, habrá que emplear estas últimas y no aquellas otras más agresivas y afectantes. Se trata, en definitiva, de la aplicación del principio de proporcionalidad".

Con todo, no ha sido sino a partir de la STC 186/2000, de 10 de julio, que se ha desarrollado con mayor claridad la forma en que debe ser jurídicamente analizada la modulación del poder de dirección del empleador, por medio de un juicio de ponderación. Esta sentencia prescribe en su fundamento jurídico 6º, lo siguiente:

"para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".

"En definitiva, como hemos señalado en la ya citada STC 98/2000 (FJ 8), el control que debe realizar este Tribunal de las resoluciones judiciales recurridas en amparo ha de recaer, precisamente en enjuiciar si, como exige la doctrina reiterada de este Tribunal que ha quedado expuesta, el órgano jurisdiccional ha ponderado adecuadamente que la instalación y empleo de medios de captación y grabación de imágenes por la empresa ha respetado en el presente caso el derecho a la intimidad personal del solicitante de amparo, de conformidad con las exigencias del principio de proporcionalidad".

Las dos sentencias precedentemente reseñadas, constituyen una pauta para la resolución de los conflictos de derechos fundamentales en el ámbito laboral, y la utilización del test de proporcionalidad se ha extendido en el ámbito judicial europeo, y por su influencia en latinoamérica.

Supone un método de resolución consistente en evaluar el impacto de la medida empresarial que aparece en confrontación con un derecho fundamental del trabajador, para finalmente deliberar si el sacrificio jurídico que sufre una de las partes, presenta una justificación razonable.

Vale precisar que dichos casos revisados, corresponden a la vulneración del derecho a la intimidad, y no invocándose directamente el derecho a la protección de datos personales, en su faz positiva o de autodeterminación informativa.

Se advierte que el conjunto de normas que regulan el tratamiento de protección de datos, en las que se invocan derechos y principios específicos, podrían llegar a suponer un mecanismo alternativo de resolución jurídica, basado específicamente en el análisis de los presupuestos y condiciones de licitud a que debe sujetarse el responsable de tratamiento de datos.

Pero dicho mecanismo de resolución, que en la especie supondría un ejercición de subsunción de reglas de licitud, implicaría desconocer que se está ante una situación de confrontación de derechos fundamentales.

Desde esta perspectiva, resulta posible declarar que el derecho a la protección de datos constituye un mandato de optimización, es decir, conforme a la conceptualización doctrinal, ordena que algo sea realizado en la mayor medida posible, dentro de las posibilidades jurídicas y reales existentes [31]

Por lo tanto, encontrándose en colisión dos derechos fundamentales, la resolución pasa por determinar qué derecho tiene más peso, o bajo qué circunstancias un derecho prevalece sobre otro.

En este sentido, la STC 39/2016, de 3 de marzo, bajo una circunstancia de conflicto entre el ejercicio del poder empresarial y el derecho a la protección de datos personales, describió en su fundamento juridico 4, el ejercicio de ponderación que se debe realizar, en los siguientes términos:

"Debe ponderarse así el derecho a la protección de datos y las eventuales limitaciones al mismo justificadas en el cumplimiento de las obligaciones laborales y las correlativas facultades empresariales de vigilancia y control reconocidas en el art. 20.3 del texto refundido de la Ley del estatuto de los trabajadores, en conexión con los arts. 33 y 38 CE. En efecto, la relevancia constitucional de la ausencia o deficiencia de información en los supuestos de videovigilancia laboral exige la consiguiente ponderación en cada caso de los derechos y bienes constitucionales en conflicto; a saber, por un lado, el derecho a la protección de datos del trabajador y, por otro, el poder de dirección empresarial imprescindible para la buena marcha de la organización productiva, que es reflejo de los derechos constitucionales reconocidos en los arts. 33 y 38 CE y que, como se ha visto, en lo que ahora interesa se concreta en la previsión legal ex art. 20.3 del texto refundido de la Ley del estatuto de los trabajadores que expresamente faculta al empresario a adoptar medidas de vigilancia y control para

[31] ALEXY, R., *Teoría de los derechos fundamentales,* Ed. Centro de Estudios Políticos y Constitucionales, Madrid, 2014, pag. 67.

verificar el cumplimiento por los trabajadores de sus obligaciones laborales (SSTC 186/2000, de 10 de julio, FJ 5, y 170/2013, de 7 de octubre, FJ 3). Esta facultad general de control prevista en la ley legitima el control empresarial del cumplimiento por los trabajadores de sus tareas profesionales (STC 170/2013, de 7 de octubre, y STEDH de 12 de enero de 2016, caso Barbulescu v. Rumania), sin perjuicio de que serán las circunstancias de cada caso las que finalmente determinen si dicha fiscalización llevada a cabo por la empresa ha generado o no la vulneración del derecho fundamental en juego".

Así entonces, en el catálogo de los derechos fundamentales inespecíficos del ámbito sociolaboral, la intimidad y privacidad tendrán una mayor presencia con respecto de la protección de datos, pero, constituyendo la relación laboral un espacio de intercambio constante de datos personales, el empleador podrá efectuar el tratamiento de dichos datos, limitadamente, cuando se trate de materias comprendidas en las obligaciones que derivan del contrato de trabajo, o bien, mediante un procedimiento que implique proporcionalidad y ponderación.

Ahora bien, el RGPD configura con particular atención la protección de datos personales en el empleo, puesto que conforme a lo dipuesto en su artículo 88 y Considerando 155, la gestión empresarial queda sometida a una organización del trabajo que garantice el respeto por la dignidad humana, y entre otros derechos, se enfatiza el resguardo de los datos del trabajador, llamando a los Estados miembros a complementar sus disposiciones legislativas o convenios colectivos para alcanzar dicho objetivo.

En este nuevo escenario, con la entrada en vigor del RGPD, el ejercicio de la ponderación tiene un cauce definido por la aplicación de los principios que rigen el tratamiento de datos personales, particularmente la limitación de la finalidad o propósito enunciada en el artículo 5.1.b). La limitación de la finalidad es una condición esencial para el procesamiento de datos personales y un requisito previo para aplicar otros requisitos de calidad de datos.

Al tenor de la disposición reglamentaria, los datos personales serán tratados con fines determinados, explícitos y legítimos, y no serán usados ulteriormente de manera incompatible con dichos fines. El ejercicio del tratamiento de datos en dichos términos resulta esencial para alcanzar la transparencia, seguridad jurídica y previsibilidad.

La aplicación de la limitación en la finalidad del tratamiento en el ámbito laboral contribuye a que el trabajador no se vea sorprendido con un uso de sus datos personales para fines inesperados, inapropiados, u objetables en otros términos.

Como contrapartida, se tolera el uso de datos para fines compatibles como herramienta de flexibilidad en el tratamiento.

Bajo este criterio el tratamiento de la imagen del trabajador, mediante fotografías, podría resultar válido en la medida que su propósito se externalice, se comunique, se revele, para que no exista ambigüedad en cuanto la intención. A modo de ejemplo, la fotografía podría ser requerida para la identificación de un empleado que efectúa atención directa al público, con el propósito de informar a la clientela quién le está brindando atención, en tanto se satisfaga además la condición de legitimidad en el tratamiento.

Para estos efectos, el concepto de legitimidad resulta más amplio que aquel establecido en el artículo 6 del RGPD, para determinar la base de licitud del tratamiento, debiendo cumplir otras disposiciones legales, ya sean de ámbito comercial, laboral, protección del consumidor, etc.

Entonces, con el objetivo de determinar si un propósito en particular se encuentra dentro de los límites de la ley, se puede recurrir a otras fuentes como costumbres, códigos de conducta, códigos de ética, arreglos contractuales, y el contexto general. De cualquier manera, las condiciones de legitimidad de un propósito son de carácter dinámico, es decir, que pueden cambiar en el tiempo a causa de desarrollos tecnológicos y cambios culturales.

Regresando al ejemplo del uso de fotografías, la legitimidad del propósito podría venir otorgada por la anuncidad necesidad de informar al cliente quién lo atiende, u otra razón posterio compatible, como la seguridad.

Entonces, el trabajador adquiere un rol protagónico al otorgársele el carácter de interesado dentro de la materialización de un tratamiento de datos. En tanto que el empleador asume el carácter de responsable, lo que supone un despliegue continuo de resguardo de los datos del trabajador, mediante acciones incorporadas a la gestión permanente de la empresa.

Sabido es que la celebración de un contrato de trabajo no implica para el trabajador la renuncia a sus derechos que –como ciudadano– le ha reconocido la Constitución, y que las empresas no conforman mundos paralelos a la sociedad, ni que mucho menos la libertad de empresa consagrada en el artículo 38 de la CE, habilite al despojo de tales derechos. [32]

Por lo anterior, la normativa sobre protección de datos personales tiene plena aplicación en el contexto de las relaciones laborales, sobretodo considerando que incluso antes de la celebración del contrato de trabajo puede efectuarse un tratamiento que podría extenderse más allá del término de la relación laboral.

Ahora bien, el tratamiento de datos personales en el ámbito laboral presenta particulares condiciones, especialmente en lo referido a la conformación de la bases jurídicas de licitud definidas en el artículo 6 del RGPD, puesto que, atendido el desequilibrio estructural en el poder negociador de las partes, el consentimiento del trabajador resulta despotenciado como fundamento de licitud, a no ser que los trabajadores puedan negarse a otorgarlo sin consecuencias adversas.[33]

Y es por tanto que, en ese sentido, las normas de protección de datos personales pasan a constituir una herramienta instrumental para la garantía de los derechos fundamentales en el trabajo.

Dicho desarrollo argumentativo lleva a que en la actualidad el empresario no puede desatender la expectativa de privacidad del trabajador con base en una decisión unilateral fundada en su poder de dirección de la relación laboral.

---

[32] STC 88/1985, de 19 de julio.

[33] Grupo de Trabajo sobre Protección de Datos del Artículo 29, Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, de 08 de junio de 2017.

III. EL TRATAMIENTO DE DATOS PERSONALES: CONCEPTOS ESENCIALES

A. El dato personal como extenso objeto de regulación

La normativa europea define dato personal como "toda información sobre una persona física identificada o identificable". [34]

En términos equivalentes, la legislación chilena[35] entiende por datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables. En la misma dirección, el proyecto de ley chileno mantiene dicha esencia terminológica al conceptualizar como "cualquier información vinculada o referida a una persona natural identificada o identificable".

Cabe puntualizar que se estima más apropiado el adjetivo "toda", pues se corresponde con el sentido de no excluir ninguna categoría o clase. A la vez, desde el punto de vista de la aplicación efectiva de la norma y su futura interpretación, sería conveniente mantener la concordancia terminológica y así aprovechar los precedentes doctrinales y jurisprudenciales que derivan de la normativa europea.

Así, a juicio del Grupo de Trabajo del artículo 29 en su Dictamen 4/2007, la expresión "toda información" indica con claridad la voluntad del legislador de dar un sentido amplio al concepto *datos personales,* por lo que tal redacción exige una interpretación extensiva.

Junto a lo anterior, cabe señalar que el sentido de totalidad de la información puede ser abarcado desde tres puntos de vista: de la naturaleza, del contenido y del formato o soporte.

En cuanto a la naturaleza, el concepto de datos personales incluye tanto informaciones de tipo objetivo (fecha de nacimiento), como subjetivo (opiniones o evaluaciones). En el ámbito de las relaciones laborales, las valoraciones de carácter subjetivo componen un amplio caudal de datos, desde la entrevista de selección de pesonal y pasando por las constantes evaluaciones formales o informales sobre desempeño.

Cabe precisar que la información no requiere que sea verídica o exacta para llegar a constituir dato personal, pues el propio sistema normativo contempla los derechos y recursos para su rectificación o supresión.

Desde el punto de vista del contenido, se incluyen todos aquellos datos que proporcionan información cualquera sea la clase de ésta, desde aquellos datos considerados sensibles hasta aquellos de carácter general, que han sido generados en cualquier ámbito de la vida de las personas, no solo dentro de su espectro de privacidad sino también en sus relaciones como ciudadano, consumidor, trabajador, etcétera.

En lo relativo al formato o soporte en que la información está contenida, se entiende comprendida cualquier forma, sea ésta alfabética, numérica, gráfica, fotográfica o fonográfica. En síntesis, resulta irrelevante el contenedor del dato, pudiendo ser digital o analógico, esté o no recogida en una base de datos o fichero estructurado.

---

[34] Dada la coincidencia conceptual existente entre el RGPD y la Directiva 95/46/CE, mantienen validez doctrinal los informes realizados en esta materia por el Grupo de Trabajo del artículo 29, principalmente en Dictamen 4/2007, de 20 de junio.

[35] Ley Nº 19.628, de 28.08.1999, artículo 2º letra f)

Esta última explicación, permite concluir que los datos biométricos son datos personales, al igual que las muestras de ADN. Por el contrario, la obtención, almacenamiento y el uso de muestras de tejido humano no constituyen dato personal, a menos que se utilicen para extraer información que permita identificar a una persona.[36]

En cuanto al segundo componente de la defición de dato personal, la preposición "sobre", tiene una función relacional, referida al vínculo entre la información obtenida y la persona que es su titular.

Existen ocasiones en las que resulta más difícil advertir el vínculo, por ejemplo, si en una fábrica se efectúa un inventario de los uniformes de los trabajadores, a primera vista se registraría un dato referido a un objeto, a menos que luego podamos saber que dicha indumentaria corresponde a un determinado trabajador y, a partir de eso, poder conocer su complexión.

Por eso es que el Grupo de Trabajo ha sostenido que "dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se trata o se evalúa".[37]

Entonces, se distinguen tres condiciones alternativas para afirmar que determinada información versa "sobre" una persona: contenido, finalidad y resultado.

El elemento contenido está presente cuando se proporciona información de una persona concreta, sin ningún propósito específico y sin esperar un resultado o repercusión de esa información en el interesado.

Por su parte, el elemento finalidad existe cuando los datos se utilizan o utilizarán probablemente, con el propósito de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona.

Por último, el elemento resultado se manifiesta, conjunta o separadamente de los demás elementos cuando es probable que su uso repercuta en los derechos e intereses de determinada persona, resultando suficiente que dicha persona pueda ser tratada diferente a causa del tratamiento de datos.

El concepto de dato personal, tal como se ha señalado, exige un vínculo relacional entre la información y un sujeto determinado o determinable que será el interesado. En razón de la importancia de definir el rol de interesado, el mismo artículo 4.1 del RGPD informa que "se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador".

Conforme al mismo reglamento, el identificador puede consistir en un nombre, un número de identificación, datos de localización, un identificador en línea o, uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Ahora bien, mediante el uso de seudónimos se pretende ocultar la identidad, pero sin embargo, podrían quedar rastros que permitan relacionar a la persona con la

---

[36] ORELLANA CANO, A.M., *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores,* Ed. Aranzadi, Pamplona, 2019, pag. 75.

[37] Documento de trabajo sobre las cuestiones relativas a la protección de datos relacionadas con la tecnología RFID, adoptado el 19.1.2005, pag. 8.

información, ya sea mediante listas de correspondencia o algoritmos criptográficos bidireccionales.

Así, cuando sea necesario, las medidas técnicas y organizativas que se adopten pueden ser claves para alcanzar una efectiva anonimización, caso en el cual no se estaría en presencia de un tratamiento sometido a la normativa de protección de datos personales.

Entonces estaremos en presencia de datos anonimizados, en el caso de aquellos que previamente permitían identificar a una persona, pero que por la aplicación de un conjunto de medios técnicos razonablemente utilizados actualmente no permiten identificar a la persona física a la que se refiere la información.

El cuarto elemento de la defincíon de dato personal, está referido a que la protección normativa se aplica a las personas física (naturales, según la legislación civil chilena). Se sigue así el sentido expuesto en el artículo 6 de la Declaración Universal de los Derechos Humanos, en que se afirma "todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica".

Ahora bien, la personalidad jurídica se entiende como la capacidad de que están dotadas las personas para ser sujetos de relaciones jurídicas, desde su nacimiento hasta su muerte, razón por la que en principio los datos personales están referidos a seres humanos vivos, identificados o identificables.

Entonces, por definición, la protección de datos no se aplica a las personas fallecidas, sin embargo, en ciertos casos, determinada información podría vincularse a datos personales que gozan de protección, ej: Madre muerta portadora de gen de la hemofilia, concedería información sobre la condición de salud de su hijo al tratarse de una condición genética hereditaria.

Por tal razón, lo recomendable sería en principio que el tratamiento de datos de personas muertas se efectúe bajo las mismas prevenciones que tratándose de vivos. Asimismo, los Estados estarían habilitados para extender mediante su legislación interna un régimen de protección de datos en favor de fallecidos, amparándose por ejemplo en un interés legítimo que lo justifique.

A modo de ejemplo, en diciembre de 2019, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos Personales de México, autorizó otorgar acceso al expediente clínico de una mujer fallecida en el parto y de su hijo recién nacido, en razón de que los documentos contienen información relacionada con la salud y el tratamiento del niño. En este caso se hizo prevalecer el interés superior del niño, considerando que el acceso a la ficha médica de su madre le abría la puerta para el ejercicio de otros derechos como la protección de la salud. [38]

En síntesis, conforme a la amplia definición contenida en RGPD sucede que prácticamente toda información referida a un trabajador entra dentro de la calificación de datos personales, y por tanto queda sometida a las normas de protección de datos.

[38] INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Comunicado, Ciudad de México, 2019. Disponible en: http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-520-19.pdf

B. El dato personal sensible: especialmente vulnerable en la relación laboral

El considerando 51 del RGPD que llama enfáticamente a otorgar una especial protección a aquellos datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y libertades fundamentales "ya que en el contexto de su tratamiento podrían entrañar importantes riesgos para los derechos y libertades fundamentales".

El artículo 9 del RGPD establece la prohición del tratamiento de datos personales obtenidos bajo ciertas condiciones o cuyo contenido exige un mayor resguardo frente a cualquier atentado o divulgación. Específicamente, corresponden a estas categorías especiales: el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

La actual legislación chilena define como datos sensibles, aquellos datos personales que se refieren a las caracterísiticas físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual. [39]

Asimismo, el marco normativo actual impide el tratamiento de datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares. [40]

Se advierte que el legislador ha pretendido otorgar mayor resguardo a los datos sensibles, por tratarse de datos personales que se refieren a las características físicas o morales de las personas, o a hechos o circunstancias de su vida privada o intimidad, y que por tanto, están expuestos en mayor medida a que el tratatamiento lesione derechos fundamentales. [41]

Ahora bien, el proyecto de ley en tramitación en el Congreso chileno [42], entiende por datos sensibles aquellos datos personales que revelen el origen étnico o racial, la afiliación política, sindical o gremial, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.

Junto a tal concepto, el nuevo marco normativo en gestación, fija una regla general para el tratatamiento de datos personales sensibles (art. 16), al indicar que solo puede realizarse cuando el titular a quien conciernen estos datos manifiesta su consentimiento

---

[39] Ley Nº 19.628, de 28.08.1999, artículo 2 letra g).

[40] Ley Nº 19.628, de 28.08.1999, artículo 10.

[41] VIOLLIER, P., *El estado de la protección de datos personales en Chile,* Derechos Digitales, Santiago de Chile, 2017. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

[42] Proyecto de Ley que modifica la Ley Nº 19.628, sobre protección de la vida privada, según texto contenido el Primer Informe de Comisión del Senado de 14.03.2018, págs 579 y siguientes. Disponible en https://www.camara.cl/verDoc.aspx?prmID=20261&prmTIPO=INFORMEPLEY,

en forma expresa, otorgado a través de una declaración escrita, verbal, o por medio tecnológico equivalente.

No obstante lo anterior, el nuevo modelo de protección de datos personales sensibles, siguiendo la ruta del RGDP, contempla un amplio margen de posibilidades para efectuar el tratamiento de estos datos aún sin contar con el consentimiento del interesado.

Así, podemos sintetizar que el tratatamiendo de datos sensibles podría llegar a ser permisible en el ámbito de las relaciones laborales, en razón de una finalidad legítima, como por ejemplo las relaciones que deriven de su afiliación sindical, o bien, para el ejercicio de un derecho o el cumplimiento de una obligación por parte del responsable del tratatamieno o el titular de los datos. Como veremos, en el ámbito de las relaciones de trabajo, el consentimiento del interesado adolece de validez suficiente como base jurídica de legitimación del tratamiento de datos personales, fundamentalmente a causa del contexto de desequilibrio entre los contratantes.

A modo de ejemplo, podemos considerar que en ciertos casos la vigilancia de la salud podría resultar obligatoria en virtud de lo dispuesto en el artículo 22.1 de la Ley de Prevención de Riesgos Laborales, ante los siguientes casos:

- Reconocimientos imprescindibles para evaluar los efectos de las condiciones laborales sobre la salud de los trabajadores.

- Verificar si el estado de salud de un trabajador puede suponer un peligro para él y otras personas, ya sean otros trabajadores o personas relacionadas con la empresa.

- En los casos que la ley obliga para la protección de riesgos específicos y tratándose de actividades de especial peligrosidad.

Con prescindencia de si el reconocimiento es voluntario u obligatorio, la base de licitud para dicho tratamiento de datos personales, consistiría en la ejecución del contrato de trabajo, circunstancia contemplada en el artículo 6.1 b) del RGPD. Cabe insistir, que de cualquier manera este tratamiento se somete al principio de limitación de la finalidad, en términos que dichos propósitos deben ser explicitados al trabajador, resguardándose un criterio de proporcionalidad que se manifiesta en que solo se pueden recoger datos necesarios para la satisfacer la necesidad de prevención.

La distinta naturaleza de los datos personales que se manejan en el ámbito laboral determina que los mismos sean objeto de un tratamiento diferenciado. Ello supone que estos datos no deben ser tratados si no son necesarios para una finalidad legítima. Los datos referidos al origen racial y vida sexual presentan escasa relevancia laboral, dado que no es fácil imaginar supuestos en los que alguno de estos datos se revele como condición de aptitud para el cumplimiento de las obligaciones derivadas de la relación laboral. Distinto es el caso de los datos referidos a la afiliación sindical, o que afectan a la salud, donde el empresario sí puede necesitar recabar y tratar informaciones relativas al descuento de cuota sindical o para dar cumplimiento a las obligaciones legales impuestas en materia de prevención de riesgos laborales. [43] [44]

---

[43] MONEREO PÉREZ, J.L. Y FERNÁNDEZ BERNAT, J.A., "Listas negras de trabajadores conflictivos (a propósito de la STS de 12 de noviembre de 2015)", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Nº 16, 2016, págs. 83-95.

[44] MERCADER UGUINA, J., "Protección de datos y relaciones laborales: apuntes prácticos sobre la entrada en vigor del Reglamento (UE) 2016/679", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Nº 41, 2018, págs. 113-126.

La Dirección del Trabajo de Chile, mediante los Dictámenes Nº 823/20 de 26.02.2003 y Nº 1085/10, de 26.03.2019, en el ejercicio de su función legal de interpretación de la legislación laboral, analiza las consultas planteadas por organizaciones sindicales referidas a la posibilidad de acceder a datos personales de los trabajadores que representa mediante requerimiento directo al empleador.[45] [46]

En la primera de las situaciones, el sindicato consulta si resulta jurídicamente procedente que una organización sindical requiera del empleador información relativa a las remuneraciones que perciben sus afiliados, para los efectos de estudiar un eventual aumento de la cuota sindical, así como la obtención de beneficios sociales para dichos afiliados.

Para la emisión de su respuesta, el órgano fiscalizador analiza el alcance de dos funtes jurídicas, la primera de ellas referida a las funciones de la organización sindical, y la segunda consistente en el deber de reserva que recarga en el empleador respecto a los datos personales de los trabajadores.

Así, se argumenta en el sentido que entre las funciones de los sindicatos destacan *"la prestación de ayuda a sus asociados, en la constitución o concurrencia a la constitución o asociación a mutualidades, fondos u otros servicios y participar en ellos, así como la constitución o concurrencia a instituciones de carácter previsional o de salud; fines éstos que necesariamente redundarán en beneficios sociales para sus afiliados".*

Seguidamente, se toma en consideración el contenido del artículo 154 bis del Código del Trabajo, al disponer que: *"El empleador deberá mantener reserva de toda la información y datos privados del trabajador a que tenga acceso con ocasión de la relación laboral".* [47]

En cuanto a esta última norma, se dice que constituye una materialización de la garantía constitucional que consagra el respeto y protección de la vida privada, pero que de ningún modo puede ser entendida como una restricción al derecho de las organizaciones sindicales a conocer la nómina de remuneraciones de sus afiliados, toda vez que aquellas actúan en cumplimiento de las finalidades que le son propias. [48]

Entonces, aunque no se utilice la actual terminología de interés legítimo para el tratamiento de datos personales, la Dirección del Trabajo recoge dicho criterio al resolver y disponer que resulta jurídicamente procedente que el directorio de la organización sindical requiera de su empleador información relativa al monto de las remuneraciones percibidas por sus afiliados, tanto para los efectos de estudiar el aumento de la cotización sindical como para la consecución de beneficios sociales para aquéllos.

---

[45] Dictamen 823/20, de 26.02.2003, disponible en: https://www.dt.gob.cl/legislacion/1624/w3-article-62851.html

[46] Dictamen 1085/10, de 26.03.2019, disponible en: https://www.dt.gob.cl/legislacion/1624/w3-article-116671.html

[47] Cabe tener presente que el artículo 154 bis del Código del Trabajo se incorporó mediante Ley Nº 19.759, vigente a partir de diciembre de 2001, momento en que la normativa sobre protección de datos personales evidenciaba un desarrollo legislativo incipiente, ya que la ley de protección de datos (Ley Nº 19.628) se había promulgado un par de años antes.

[48] El análisis de la garantía constitucional se centra exclusivamente en el Derecho a la Privacidad, puesto que el Derecho a la Protección de Datos solo alcanzaría rango constitucional en el año 2018.

Por otra parte, el segundo y más reciente pronunciamiento jurídico (Dictamen Nº 1085/10, de 26.03.2019), tiene la particularidad de haberse emitido en un contexto en que el Derecho a la Protección de Datos Personales ha sido recientemente incorporado a la Constitución chilena, y estando vigente el RGPD en Europa (que como se ha analizado en el Capítulo II sirve de modelo en su contenido jurídico).

En este Dictamen, el empleador requiere un pronunciamiento jurídico sobre la procedencia de entregar a la organización sindical información sobre sus afiliados, en particular aquella relativa a: remuneraciones mensuales, resultados de evaluaciones de desempeño, registro de entrada y salida de labores, aumentos de rentas, entre otros.

Sobre el particular, cabe considerar en primer término que los datos requeridos por la organización sindical, si bien, constituyen datos personales, no revisten el carácter de dato sensible, por lo que su tratamiento está sometido a las normas generales de protección de datos personales.

Se advierte que el órgano administrativo laboral, en su pronunciamiento, centra su análisis respecto al tratamiento de la información dentro de la esfera del Derecho a la Privacidad, apreciándose la confusión semántica entre "datos privados" y "datos personales".

Si bien es cierto que el artículo 154 bis del Código del Trabajo, establece la reserva de toda información y datos privados del trabajador, aquella no puede ser entendida como secreto de los datos, sino que al amparo de la normativa de protección de datos personales, cabe entender la reserva como manifestación del principio de responsabilidad proactiva del responsable de tratamiento de datos.

Así, resulta evidente que la omisión del análisis del contenido del Derecho Constitucional de Protección de Datos –incorporado a la Carta Fundamental en 2018–, ha derivado en una conclusión que se aparta de los actuales fines y propósitos de la normativa de protección de datos, al resolver que:

"1. Para que una organización sindical representando debidamente a uno de sus trabajadores afiliados -en cumplimiento de las finalidades que le son propias- exija información o datos privados de aquel trabajador a su empleador, quien la posee con ocasión de la relación laboral que lo vincula con aquel, deberá encontrarse autorizada expresamente por dicho trabajador. De contar con dicha autorización, no resultaría aplicable lo dispuesto en el artículo 154 bis del Código del Trabajo, pues aquella organización sindical no actúa a nombre propio, sino en representación y autorizada por el titular de dicha información, es decir el trabajador. Complementa Dictamen Ordinario N° 823/20 de 26.02.2003".

"2. El ejercicio de los distintos tipos de derecho a información conferidos a las organizaciones sindicales en el Título II del Libro IV del Código del Trabajo, no obsta a que dichas organizaciones soliciten, en virtud de su poder de representación de sus trabajadores afiliados y en los términos antes expuestos, información o datos privados de sus representados, pues en este último caso, dichas organizaciones no actúan como titulares, sino a nombre y en lugar de dichos trabajadores".

De esta forma, conforme al actual criterio de la Dirección del Trabajo en Chile, el tratamiento de datos por parte de la organización sindical, solo tendría validez cuando la base jurídica consista en el consentiemiento expreso del trabajador, pues se trataría de "datos privados" que solo él puede disponer en cuanto a su traspaso o tratamiento.

Entonces, el segundo pronunciamiento no solo complementa el Dictamen original, sino que implica un cambio radical de criterio, desconociendo la legitimación para el tratamiento de datos de datos que recae en el sindicato en razón de los fines e intereses que persigue, lo cual, sin embargo, no obsta a que los datos a ceder a los órganos de representación deberán ser necesarios y proporcionados para la finalidad para la que se ceden, de modo que frente al requerimiento de los datos deberá aclararse la necesidad concreta para la que se necesita tal información, pues de no ser así, estaríamos ante un tratamiento desproporcionado o innecesario de dicho dato personal.

Por lo antes expuesto, la organización sindical que solicite al empleador información que constituya datos personales de sus afiliados deberá justificar la finalidad a la que va destinada dicha obtención, no bastando una genérica referencia a las funciones que le reconoce el ordenamiento jurídico, siendo exigible un análisis en relación con que la solicitud de información resulta adecuada, necesaria y proporcional al cumplimiento de la finalidad perseguida, valoración que podrá efectuar el empleador en su rol de responsable de los datos. [49]

En otro de sus pronunciamiento, la Dirección del Trabajo ha informado que tratándose de datos concernientes al estado de salud de los trabajadores, el empleador está facultado para adoptar medidas tendientes a verificar el debido ejercicio del derecho a usar de licencia médica, pero que sin embargo, la entrega a terceros de los antecedentes personales del dependiente o sus condiciones de salud, infringe el deber de confidencialidad consagrado en el artículo 154 bis del Código del Trabajo, al no revestir dicha medida el carácter de medio necesario o idóneo a la finalidad perseguida[50]. También se ha puntualizado que en la eventualidad de que un trabajador y/o postulante a un empleo consienta en otorgar información referente a su discapacidad o pensión de invalidez, los empleadores deberán guardar total confidencialidad y reserva, conforme a lo dispuesto por el artículo 154 bis del Código del Trabajo. [51]

C. Claves para la licitud del Tratamiento de Datos Personales

Conforme al artículo 4.2 del RGPD se entiende por *tratamiento* "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción". [52]

De esta manera, el tratamiento constituye el objeto jurídico de la normativa sobre protección de datos personales, misma que en cuanto a su ámbito de aplicación se

---

[49] MERCADER UGUINA, J., "Protección de datos y relaciones laborales…" *Op. Cit.*

[50] Ordinario Nº 3871 de 13 de agosto de 2019. https://www.dt.gob.cl/legislacion/1624/w3-article-117379.html

[51] Dictamen Nº 6245/047 de 12 de diciembre de 2018. https://www.dt.gob.cl/legislacion/1624/w3-article-116231.html

[52] En términos semejantes el artículo 2 letra o) de la Ley Nº 19.628, define para Chile el tratamiento de datos como: "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma".

extiende al tratamiento total o parcialmente automatizado de datos personales, como también, al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. [53]

Ahora bien, tal como lo contempla el considerando 51 del RGPD, todo tratamiento debe someterse al cumplimiento de requisitos destinados a satisfacer determinados presupuestos de licitud para llevar a cabo el tratamiento, junto a condiciones permanentes del tratamiento que permitan el ejercicio efectivo del derecho de privacidad de los afectados.

1. Los Principios para el Tratamiento de Datos Personales

Estos principios constituyen mandatos de optimización de conducta que resultan vertebradores de la legitimidad de todo sistema de tratamiento de datos. Su análisis resulta fundamental para determinar la proporcionalidad de las acciones relacionadas con el manejo de datos personales.

- Principio de licitud: Está referido a la existencia de una base jurídica que legitime el tratamiento de datos, dentro de aquellas enumeradas en el artículo 6 del RGPD. Si bien el consentimiento del interesado actuará mayoritariamente como llave habilitante, el legislador también puede reconocer otras circunstancias que habilitan al tratamiento.

- Principio de lealtad y transparencia: Se encuandra en el deber de informar con anticipación el hecho de que se efectuará el tratatamiento y los fines que este persigue. Con carácter prácticamente inseparable, la lealtad y transparencia, resaltan el deber de información respecto del alcance del tratamiento, y el rechazo al uso de medios clandestinos en la obtención de los datos.

Se advierte un debilitamiento de este principio en los casos de sospecha fundada sobre la comisión de ilícitos o conductas graves moralmente reprochables, en las que el uso de formas subrepticias de tratamiento resultan el único medio de confirmación o prueba.

- Principio de limitación de la finalidad: Conlleva la obligación de que los datos deben ser tratados con fines o propósitos legítimos y definidos explícitamente y de forma previa; secundariamente, impide que los datos sean tratados posteriormente de manera incompatible con dichos fines.

A este respecto, la Dirección del Trabajo en Chile ante la consulta de si un empleador ha de estar obligado a proporcionar datos personales de los trabajadores a la Fiscalía Nacional Económica para el estudio del mercado de medicamentos, rechazó la procedencia jurídica de dicho tratamiento solo en virtud del deber de reserva que recae en el empleador, sin considerar aspectos como la limitación de la finalidad o el principio de minimización de datos. [54]

- Principio de minimización de datos: Se traduce en que todo tratamiento de datos debe evitar acceder a información que no sea exclusivamente necesaria en función de los propósitos definidos. La limitación puede centrarse en cuatro fases: objetivo (tratamiento exclusivamente de los datos apropiados), teleológico (solamente para los fines

[53] Art 2.1 RGPD.

[54] Ordinario Nº 4935 de 17 de octubre de 2019. https://www.dt.gob.cl/legislacion/1624/w3-article-117663.html

adecuados), subjetivo (respecto exclusivamente de la persona física a que se refiera el tratamiento), temporal (por el tiempo más breve posible y necesario).

- Principio de exactitud: Los datos deben ser exactos, de lo que se infiere que deben ser rigusamente ciertos, correctos y actualizados. A este propósito los interesados deberán contar permanentemente con la posibilidad de verificar la información, y así, en caso de ser procedente, ejercer sus derechos en orden a obtener la rectificación, supresión o complementación necesaria.

En el ámbito laboral muchas veces se advierte un continuo tratamiento de los datos personales de los trabajadores, principalmente por los sistemas de monitorización, razón por la que en el ejercicio de este principio el empleador deberá actuar con sentido de transparencia y permitir la verificación periódica de la información que atañe a cada persona.

- Principio de limitación del plazo de conservación: Los datos personales deber ser mantenidos exclusivamente por el tiempo necesario para satisfacer el propósito y necesidad del tratamiento.

- Principio de integridad y confidencialidad: Este principio, comprende un aspecto técnico y otro de responsabilidad de las personas involucradas en el tratamiento de datos personales. Por una parte, se debe contar con un sistema y herramientas que proporcionen seguridad tecnológica, y también, un nivel de capacitación y refuerzo en el hacer cotidiano del deber de sigilo y confidencialidad en el manejo de la información. Todo lo anterior, está destinado a otorgar una garantía de seguridad en el tratamiento de datos personales, contra todo riesgo de pérdida, destrucción o daño; o bien, frente a un uso no autorizado o ilícito de los datos.

- Principio de la responsabilidad proactiva: Todo proceso de tratamiento de datos personales impone a su responsable el deber de garantizar y acreditar, en cualquier momento, la licitud, lealtad y transparencia de dicho tratamiento.

Este principio cobra vital importancia frente a la utilización de tecnologías que efectúen combinación de datos o desarrollen usos secundario, donde a partir del artículo 25 del RGPD se pretende una configuración de la protección de la privacidad desde el diseño y por defecto. Así, el usuario de datos deberá adoptar, previo juicio de ponderación, la medidas técnicas y organizativas más adecuadas para el cumplimiento de los principios de protección de datos y su demostración, integrándose en las prácticas empresariales directamente y en todo momento. [55]

La responsabilidad proactiva o *accountability*, apunta sobre todo al modo en que se ejercen las competencias y su forma de verificación. Entonces, la accountability debe materializarse en el reconocimiento, asunción de responsabilidad y actitud transparente sobre los impactos de las políticas, decisiones, acciones, productos y desempeño asociados a una organización. [56]

2. Bases Jurídicas para el Tratamiento de Datos Personales

Las fuentes o bases de legitimidad son aquellas hipótesis definidas por el ordenamiento jurídico que facultan para el tratamiento de datos personales.

---

[55] BAZ TEJEDOR, J.A., "Inteligencia artificial y privacidad del trabajador predictible", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Monográfico Nº 11, 2020.

[56] MERCADER UGUINA, J., "Protección de datos y relaciones laborales…" *Op. Cit.*

En otras palabras, el tratamiento de datos personales, por si eventualmente en el futuro tales antecedentes pudieran resultar útiles o justificados, sino que desde un inicio deben sujetarse a las bases de licitud que contempla el artículo 6 del RGPD.

En el contexto de las relaciones laborales, cabe describir las características particulares que asume el consentimiento, y la particular importancia de las razones de cumplimiento de una obligación contractual o precontractual, y la existencia de un interés legítimo.

Si bien, el consentimiento en la mayoría de los casos constituirá fundamento jurídico suficiente, aquello no ocurrirá cuando el tratamiento se refiera a una categoría especial de datos, o bien, cuando conforme a la naturaleza de la relación jurídica no sea presumible que el consentimiento será libremente manifestado.

El consentimiento ha sido considerado como un acto de transformación moral que modifica las expectativas normativas entre las personas y los grupos, y tiene otra parte, la capacidad de hacer pensar activamente a los individuos sobre las consecuencias de su otorgamiento. [57]

La defición de consentimiento ha evolucionado a la par de los cambios normativos, léase entre la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, ambas en compararación al actual RGPD. [58] [59]

Tales criterios han sido desarrollados en los Documentos de Trabajo y Opiniones formulados por el antiguo Grupo de Trabajo del artículo 29 (Directiva 95/46/CE) –hoy reemplazado por el Comité Europeo de Protección de Datos (artículos 68-76 RGPD)– primeramente en el Dictamen 15/2011, ampliado y complementado por la Directrices sobre el Consentimiento en el sentido del RGPD, adoptado el 28 de noviembre de 2017.

Específicamente, al tenor de lo dispuesto en el artículo 4, apartado 11, del RGPD, se entiende por consentimiento "…toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

El actual concepto contemplado en la normativa europea se ve fortalecido por un conjunto de otras disposiciones del mismo RGPD, que regulan aspectos tales como la manera de manifestar, acreditar o revocar.

---

[57] SCHERMER, B.W., CUSTERS, B., Y VAN DER HOF, S., "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection*", Ethics and Information Technology*, Nº 16, 2014, págs. 171–182. Disponible en https://doi.org/10.1007/s10676-014-9343-8

[58] El artículo 2 letra h) de la Directiva 95/46/CE, definió el consentimiento como toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

[59] Conforme al considerando 17 de la Directiva 2002/58/CE, "…el consentimiento de un usuario o abonado, independientemente de que se trate de una persona física o jurídica, debe tener el mismo significado que el consentimiento de la persona afectada por los datos tal como se define y se especifica en la Directiva 95/46/CE. El consentimiento podrá darse por cualquier medio apropiado que permita la manifestación libre, inequívoca y fundada de la voluntad del usuario…"

A la luz de la definición, además se infieren los elementos copulativos que determinan la validez de la manifestación de voluntad, la que debe ser: libre, específica, informada, e inequívoca.

El proyecto de ley de protección de datos personales en Chile declara que el consentimiento no se considerará una base jurídica suficiente para la validez del tratamiento de datos, cuando exista un desequilibrio ostensible entre la posición del titular y el responsable.

Dado lo anterior, podemos entender que en el contexto de las relaciones laborales el consentimiento ve menguada su capacidad legitimadora del tratamiento de datos personales, toda vez que consiste en un vínculo esencialmente subordinado y, por tanto, expresión del desequilibrio negociador de los contratantes.

Como contrapartida, solo procede dar por válido aquel consentimiento emitido en circunstancias cuya excepcionalidad se deduce de la ausencia de consecuencias derivadas de la aceptación o rechazo por parte del trabajador, situación difícil de imaginar en el ámbito laboral. [60]

Así, llama la atención el criterio empleado por la Dirección del Trabajo en Chile al informar como decisión que "*el trabajador puede consentir en que su empleador realice algún tipo de tratamiento de sus datos"*, pero que luego rechaza la procedencia del tratamiento porque el anexo en que se requiere la utilización de datos (voz, imagen, nombre y correo electrónico) carece de precisión para una decisión informada. En este caso la decisión administrativa no se evalúa aspectos como la escasa libertad del trabajador para manifestar su consentimiento, la imprescindible base de licitud para el tratamiento, o la proporcionalidad de la medida.[61]

En lo que respecta a la base de legitimidad consistente en el cumplimiento de una obligación contractual o precontractual, ésta resulta de vital importancia en el ámbito laboral, por los particulares intereses de las partes que derivan del contrato de trabajo, como, por ejemplo: el pago de las remuneraciones o el ejercicio del poder de dirección por parte del empleador. Asimismo, por el rol que le corresponde al empleador como gestor delegado de los poderes públicos (retención de impuestos, tramitación de licencias médicas, retenedor de cotizaciones de la seguridad social).

Tratándose de las medidas precontractuales, con motivo de una eventual relación laboral, la recopilación de antecedentes personales de quienes postulan a una oferta de trabajo, está amparada por esta base de licitud en la medida que esté en concordancia con los principios, principalmente la minimización de datos, finalidad y responsabilidad proactiva.

A modo de ejemplo, en procesos de selección, el eventual empleador que efectúe recogida de datos de los postulantes mediante la revisión de sus redes sociales, no gozaría de legitimación para dicho tratamiento.

Aun cuando se trate de fuentes de información públicas, dicho datos no han sido informados con el propósito de que sean utilizados para fines laborales. Por el contrario,

---

[60] VILLALBA SÁNCHEZ, A., "El principio de transparencia en la ejecución automatizada del contrato de trabajo: una aproximación jurídica a la tecnología "blockchain" y a la inteligencia artificial", *Nueva Revista Española de Derecho del Trabajo,* Nº 224, 2019, págs. 183-226.

[61] Ordinario Nº 5589 de 04 de diciembre de 2019. https://www.dt.gob.cl/legislacion/1624/w3-article-117890.html

el empresario podría invocar una base jurídica de licitud como el interés legítimo, debiendo someterse de paso a las demás normas de protección de datos, principalmente la limitación de la finalidad, transparencia y minimización de los datos.

En cuanto al fundamento de licitud referido a la satisfacción de un interés legítimo, se adiverte que su alcance es de carácter muy amplio, razón por la que exige una adecuada ponderación para ser invocada, es decir, que operará en la medida que resulte idónea y necesaria para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales

Una necesidad legítima, corresponde a aquella reconocida por el ordenamiento jurídico y compatible con los derechos de terceros —por ejemplo, la obtención de un provecho económico—, y susceptible de ser satisfecha mediante una o varias operaciones de procesamiento de datos. [62]

[62] CONTRERAS VÁSQUEZ, P. Y TRIGO KRAMSCSÁK, P., "Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile", *Revista Chilena de Derecho y Tecnología,* Vol. 8 Nº 1, Santiago de Chile, 2019, págs. 69-106.

IV. RESPONSABILIDAD PROACTIVA DEL EMPRESARIO: EXPECTATIVA DE GOBERNANZA FUERA DEL ESPACIO EUROPEO

A. Adopción de una cultural empresarial de protección de datos, en todo momento y a todo nivel.

La irrupción digital afecta a todo tipo de centros de trabajo, públicos o privados, autónomos o dependientes, a empresas transnacionales o pequeños talleres. Tal carácter de universalidad, posibilita analizar el fenómeno en cualquier sistema jurídico, siempre considerando que el derecho ha de ir en paralelo con el avance de las tecnologías emergentes, puesto que, la inclusión de Tics en el trabajo pueden difuminar determinados derechos laborales. [63]

Se advierte que estamos ante un momento de disolución de las estructuras jurídicas tradicionales, y por tanto, no es claro el rol del legislador en la definición de modelos normativos que deberán regir en el futuro, esto sin perjuicio de que el Derecho está compuesto por normas dinámicas, y que particularmente en el área de las relaciones laborales deben ser consensuadas por actores provenientes de diversas áreas del conocimiento y del actuar social. [64]

En este contexto, el principio de responsabilidad proactiva se erige como un cánon de conducta, que puede incluso suplir la ausencia de una norma específica. En este sentido, el artículo 25 del RGPD consagra un principio de protección de datos "desde el diseño" y "por defecto", que en síntesis exige una concepción de la privacidad como valor organizacional, por el que cada esfera del negocio asume no solo el cumplimiento de la normativa, sino que un esquema de gestión que se anticipe a cualquier vulneración del derecho.

Entonces, el RGPD introduce un modelo organizacional que, en virtud de las intensas relaciones comerciales de Chile con los países europeos, puede convertirse en estándar entre las empresas que han extendido su espacio de actividad en términos territoriales, o como prácticas de negocios respetuosas de los derechos fundamentales.

Este modelo de responsabilidad empresarial convoca a que el responsable aplique al momento de determinar los medios de tratamiento, como en el instante del tratamiento, medidas técnica y organizativas apropiadas, conforme al estado de la técnica, su costo y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas.

El punto de mayor debate que puede generar este modelo de gestión, consiste en el alcance de lo que debe entenderse como "medidas apropiadas", puesto que éstas –desde el punto de vista empresarial– podrían ser interpretadas solo en función de su factibilidad técnica o económica, y no desde el deber de proporcionalidad exigible ante la confrontación de derechos fundamentales. En estos casos, el procedimiento adecuado de

---

[63] TRUJILLO PONS, F., "La urgente necesidad de legislar el trabajo a distancia y la desconexión digital en el trabajo", *El foro de Labos,* Blog, entrada de 16.06.2020. Disponible en: https://forodelabos.blogspot.com/2020/06/la-urgente-necesidad-de-legislar-el.html

[64] MERCADER UGUINA, J., "Nuevos escenarios para el Estatuto de los Trabajadores del siglo XXI: digitalización y cambio tecnológico", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Nº 63, 2020.

resguardo consiste en aplicar primero el test de proporcionalidad y luego evaluar si se cumple la codición de las "medidas apropiadas". [65]

Por otra parte, las medidas organizativas deben estar diseñadas de manera transversal en todas las áreas de la empresa, entre ellas, finanzas. Por lo que resultará procedente la evalución de los efectos económicos que impone la gestión del tratamiento de datos personales, en particular, la reducción de costos que puede involucrar, cuando se compara frente al riesgo por sanciones o daño reputacional.

De esta manera, un correcto sistema de evaluación de riesgos, deberá considerar el impacto a nivel del prestigio empresarial, y el apoyo a la generación de nuevos negocios que puede acarrear la implementación de buenas prácticas en el tratamiento de datos personales.

De todas formas, la implementación del principio de privacidad desde el diseño, involucra la participación de los trabajadores, como miembros de la organización y en su carácter de interesados en el tratamiento de datos.

En este contexto, la negociación colectiva favorece el diálogo sobre la implementación de herramientas tecnológicas al interior de la empresa, particularmente, respecto de aquellos sistemas de control de la actividad laboral, abriendo paso al uso de medios más respetuosos de la privacidad, y cumplir de forma más participativa el deber de información sobre los fines del tratamiento.

La aplicación de medidas organizativas *ex ante*, impedirían por ejemplo el uso de plataformas tecnológicas como Teams, en tanto las mismas no se correspondan con la política de privacidad de la empresa, aspecto que se evaluaría antes de su implementación, o bien, durante el desarrollo de auditorías periódicas. En este caso el empleador, por el solo hecho de haber incorporado a la cultura empresarial un sentido de respeto por la privacidad, habría anunciado a los trabajadores (transparencia y licitud) los informes de uso que registra Teams, si se haría uso de aquellos y con qué finalidad.

Por todo lo anterior, la responsabilidad proactiva constituye el eje vertebrador del modelo europeo de protección de datos, el que puede ser seguido a nivel global por las empresas, aún a falta de normas jurídicas que las impongan.

En Chile, bajo el sistema legislativo actual, podría operar en ámbito del *soft law*, en los mismo términos que en algún momento sucedió con las reglas sobre protección del medio ambiente y que luego pasaron a constituir un deber jurídico y ético.

B. Teams de Microsoft: Trabajo en equipo pero bajo vigilancia.

A la luz de los principios y bases de licitud revisadas, podemos evaluar desde una dimensión práctica el uso de la herramienta tecnológica Teams de Microsoft, la que se presenta como una aplicación colaborativa que permite la organización de equipos de trabajo, compartir archivos y mantener comunicaciones grupales o privadas mediante chat, videoconferencias o llamadas. Desde el punto de vista de su arquitectura, se trata de un software que se ejecuta en servidores propios de la organización empresarial, o bien, mediante la utilización de hardware de microsoft, al que los usuarios se conectan en red desde cualquier lugar.

A causa de la pandemia Covid-19 y las restricciones al desplazamiento de las personas cobró vigor el teletrabajo como sistema de organización productivo, por lo que

[65] BAZ TEJEDOR, J.A., "Inteligencia artificial y privacidad…" *Op. Cit.*

muchas empresas debieron implementar herramientas tecnológicas con las que poder enfrentar este nuevo escenario. [66]

Con ese enfoque, cabe señalar que Teams ofrece a los administradores la posibilidad de acceder a datos de análisis e informes de uso[67]. Con esta herramienta, en el entendido de que quien cumple la función de administrador en una organización es el empleador o quien lo representa, se pueden obtener diversos antecedentes susceptibles de ser destinados a la evalución del desempeño laboral de los usuarios de Teams. El informe de uso de Teams, en general se refiere a cuantos usuarios de la organización utilizan la herramienta dentro de un intervalo de fechas, y el tipo de actividad que desarrollan. Puntualmente, el empleador puede conocer: nombre del equipo, número de usuarios activos en el equipo en el período de tiempo especificado, número de canales que tienen al menos un usuario activo en el período de tiempo especificado, número de todos los mensajes enviados en los canales en el período de tiempo especificado, número de todos los mensajes de respuesta en los canales en el período de tiempo especificado, número de todas las reuniones programadas que un usuario ha organizado, número de todos los mensajes urgentes en el período de tiempo especificado, número de todas las reacciones a los mensajes en el período de tiempo especificado, número de las menciones usadas en los mensajes en el período de tiempo especificado, y el número de mensajes únicos que los usuarios del equipo publicaron en un chat de equipo durante el período de tiempo especificado.

Por su parte, el informe de actividad de usuarios de Teams, permite obtener acceso a los siguientes datos: nombre para mostrar del usuario, número de llamadas de 1:1 en las que el usuario ha participado durante el período de tiempo especificado, mensajes únicos que el usuario ha publicado en un chat de equipo durante el período de tiempo especificado, número de mensajes de respuesta únicos que el usuario ha publicado en un canal de equipo durante el período de tiempo especificado, número de mensajes post únicos que el usuario ha publicado en un canal de equipo durante el período de tiempo especificado, número de reuniones programadas que un usuario organizó durante el período de tiempo especificado, número de reuniones programadas en las que ha participado un usuario durante el período de tiempo especificado, número de mensajes únicos de chat que el usuario ha publicado en una conversación privada durante el período de tiempo especificado, número de mensajes urgentes que el usuario ha publicado en una conversación durante el período de tiempo especificado. número de llamadas grupales en las que ha participado el usuario durante el período de tiempo especificado, tiempo total de audio en el que el usuario participó durante el período de tiempo especificado, tiempo total de video en el que el usuario participó durante el período de tiempo especificado, tiempo total en que el usuario ha compartido pantalla durante el período de tiempo especificado, y la última actividad (última fecha (UTC) en la que el usuario participó en una actividad de Teams).

Además, cabe tener presente que todos estos datos pueden ser exportados desde Teams en formato de archivo CSV o Excel, lo que habilita a que el empleador continúe

---

[66] ITSELLER.CL, *Coronavirus: Microsoft ofrece Teams gratuito para realizar teletrabajo.* https://www.itseller.cl/2020/03/17/coronavirus-microsoft-ofrece-teams-gratuito-para-realizar-teletrabajo/ (Revisado el 13-jun-2020)

[67] Presentación oficial de estas herramientas en la web https://docs.microsoft.com/es-ES/MicrosoftTeams/teams-analytics-and-reports/teams-reporting-reference (Revisado el 14 junio 2020).

con procesos adicionales de tratamiento, incluso derivando en la elaboración de perfiles para la adopción de decisiones automatizadas.

Se advierte entonces que Teams no solo es un canal de comunicaciones o trabajo colaborativo, sino que ofrece informes destinados al control de la actividad laboral valiéndose de los datos almacenados durante el uso de la plataforma, y sobre los que el usuario no es advertido en la defición de las caracterísiticas de la aplicación.

Vemos que Microsoft habilita la emisión de informes, que pueden ser destinados al control de las obligaciones contractuales, pero que no han sido requeridos por los empresarios, y sin que tampoco se verifique previamente que otros sistemas de supervisión, menos instrusivos, permitan obtener el resultado de rendimiento o productiva razonablemente esperado.

El trabajador que utiliza la plataforma Teams, lo hace bajo el entendido que se trata de una plataforma de trabajo colaborativo, y que esencialmente ofrece herramientas de comunicación e intercambio de información.

En el caso que el empleador quisiera invocar como base jurídica de licitud del tratamiento, previamente tendría que someterse al examen sobre limitación de la finalidad, base sobre la cual poder realizar la prueba de proporcionalidad de forma previa a la utilización de la plataforma.

Lo anterior, obliga conjuntamente a efectuar una comunicación efectiva a los trabajadores, en virtud del principio de transparencia. Dicha comunicación debiera dar a conocer en forma clara, según el nivel de conocimientos de cada usuario, los fines que persigue el tratamiento de datos, como también, la legitimidad de que gozan tales propósitos.

Bajo otro escenario, en el que el empleador invoque una base jurídica legítima, como podría ser el cumplimiento de las obligaciones que derivan del contrato de trabajo, en circunstancias excepcionales de pandemia, es necesario advertir que los informes emitidos implican un control sobre el desempeño laboral, que se efectúa permanentemente respecto tanto de las actividades ejecutadas en la plataforma como también respecto de los períodos de inactividad, resultando en definitiva de una alta intensidad frente al resguardo de la intimimidad del trabajador, implicando una invasión a su privacidad en el entorno laboral, excediendo todo criterio de proporcionalidad.

V. EL TRABAJADOR CHILENO: INJUSTAMENTE A LA DERIVA

Mediante la entrada en vigencia de la Ley Nº 19.628 sobre Protección de la Vida Privada[68], Chile se convirtió en el primer país latinoamericano en contar con una legislación sobre la materia.

Sin embargo, en la normativa vigente se advierten importantes errores que han impedido su real eficacia. Se le reclama la falta de un registro de bases de datos particulares, un ente fiscalizador, un procedimiento de reclamación y un régimen sancionatorio efectivo. En términos globales, ha transformado el habeas data en una declaración de buenas intenciones, frente a una enorme libertad para el tratamiento de datos incluso sin autorización de sus titulares. [69]

Dentro de la normativa laboral, el Código del Trabajo contempla en su artículo 154 bis, una vinculación directa con la protección de datos personales en el trabajo, al prescribir:

"El empleador deberá mantener reserva de toda la información y datos privados del trabajador a que tenga acceso con ocasión de la relación laboral".

Además, este escaso régimen destinado a la protección de la intimidad del trabajo se complementa con el inciso primero del artículo 5º, que aunque de un contenido más general, resulta aplicable a la materia, al señalar que:

"El ejercicio de las facultades que la ley le reconoce al empleador, tiene como límite el respeto a las garantías constitucionales de los trabajadores, en especial cuando pudieran afectar la intimidad, la vida privada o la honra de éstos". [70]

La aplicación de la Ley 19.628, así como los artículos 5º y 154 bis del Código del Trabajo, contribuyen a brindar amparo a los derechos fundamentales de los trabajadores, por la vía de garantizar la autodeterminación informativa del titular de los datos.

Con todo, la normativa antes referida no resulta suficiente para prever soluciones jurídicas apropiadas respecto de la protección al afectado por el tratamiento de datos personales en el contexto de las relaciones de trabajo. [71]

A pesar de lo anterior, resulta fundamental el rol de la Dirección del Trabajo, que en ejercicio de su facultad de interpretación de la legislación laboral, ha dado contenido y eficacia a tan escueto régimen normativo. En este punto, llama la atención que a más de dos años de vigencia de la norma constitucional que incorporó el derecho a la

---

[68] Publicada en el Diario Oficial del 28 de agosto de 1999.

[69] JIJENA LEIVA, R., "Actualidad de la Protección de Datos Personales en América Latina. El caso de Chile", Ibarra Sánchez, E. y Téllez Valdes, J. (Cords), *Memorias del XIV Congreso Iberoamericano de Derecho e Informática*, tomo 1, Universidad Autónoma de Nuevo León, México, 2010. Disponible en: https://biblio.juridicas.unam.mx/bjv/detalle-libro/2940-memorias-del-xiv-congreso-iberoamericano-de-derecho-e-informatica-t-1

[70] Cabe observar que tanto el inciso 1º del artículo 5º y el artículo 154 bis del Código del Trabajo, por la Ley Nº 19.759 de 05 de octubre de 2001, lo que evidencia que a principios del siglo XXI el legislador tuvo particular interés por la protección datos de los trabajadores, sin que posteriormente se mantuviera dicho énfasis normativo.

[71] CERDA SILVA, A., "Intimidad de los trabajadores y Tratamiento de datos personales por los empleadores", *Revista de Derecho Informático*, Nº 2, Santiago de Chile, 2003. http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_completo/0,1492,SCID%253D14643%2526ISID%253D292,00.html#

protección de datos personales al catálogo de derecho fundamentales, ninguno de los pronunciamientos emitidos por la Dirección del Trabajo ha invocado dicho precepto, manteniendo solo la referencia a los derechos de intimidad o privacidad de los trabajadores.

Sin embargo, lo anterior se entiende en función del sentido que ha adoptado la jurisprudencia de la Corte Suprema, que lejos de darle aplicación al derecho fundamental de protección de datos, ha desconocido su vigencia, en tanto que el legislador no efectúe un desarrollo amplio de los principios y derechos que actualmente reconoce el sistema normativo europeo, al ser éste su fuente directa.

Finalmente, el proyecto de ley en tramitación debe forzosamente considerar el desarrollo y concreción de principios como el consentimiento y finalidad, la transparencia y la responsabilidad proactiva.

Conjuntamente, se debe incorporar un apartado de normas específicas para la situaciones de tratamiento de datos en el ámbito laboral, que asegure la participación de las organizaciones sindicales ante la adopción de medidas de control por parte del empleador; y definir el rol que tendrá la Dirección del Trabajo en la fiscalización de esta materias, o si por el contrario tales facultades serán asumidas exclusivamente por la autoridad protectora de datos.

VI. CONCLUSIONES

Hoy se ha instalado una pseudoverdad entre quienes transitan los mundos de lo jurídico y lo tecnológico, que niega la opción a reclamar el respeto por la privacidad, admitiéndose exclusivamente que las personas controlen el uso lícito de los datos que les conciernen.

Supuestamente, de mantener inamovible el cerco de lo privado obstaculizaríamos el desarrollo o renunciaríamos a los benecificios sociales que acarrean tecnologías como big data o inteligencia artifical.

Pero la privacidad aún constituye un reducto de libertad, un espacio para la creación y la expresión del pensamiento, del que han derivado la mayoría de los progresos de la humanidad. La persona que se sabe observada modifica su comportamiento, para someterse a las reglas de lo socialmente aceptado o permisible.

En esta etapa, lo jurídico tiene el rol de modular ambas perspectivas mediante la construcción de un sistema de gobernaza global, aspecto en que el sistema europeo tiene un importante camino adelantado, particularmente mediante las directrices de repsonsabilidad proactiva.

La evolución del cuerpo normativo sobre la protección de datos personales, que he presentado en el desarrollo de este trabajo, ofrece hoy en el RGPD un modelo evolucionado y con respaldo institucional para su adecuada aplicación, del que se ha pretendido esbozar sus ideas estructurantes.

Chile ha retomado el camino normativo para ofrecer un escenario que promocione y salvaguarde la privacidad, mediante el reconocimiento constitucional del derecho a la protección de datos personales, y la tramitación de un proyecto de ley que moderniza la legislación sobre esta materia, siguiendo el modelo europeo, según ha sido verificado en los apartados respectivos.

Entonces, podemos asegurar que el contenido que corresponde asignar a las normas de protección de datos personales en Chile, no es otro que el adoptado en el espacio europeo, por parte del TEDH y los tribunales superiores de España, país con el que se mantiene una larga tradición jurídica, y que se ha tenido como referente en la durante la actividad legislativa.

Por tanto, el criterio sostenido por la Corte Suprema de Chile consistente en que el derecho a la protección de datos personales –consagrado a nivel constitucional– exige un desarrollo legislativo adicional, produce un injustificado vaciamento del derecho fundamental, puesto que aquel podría ser aplicado siguiendo el contenido esencial descrito por la doctrina y jurisprudencia europea. No hay duda que otros aspectos como la actividad fiscalizadora, sanciones, o procedimiento específico de reclamación, exigen un desarrollo a nivel legal, pero en ningún caso se puede admitir el cercenamiento de un derecho fundamental por ausencia de texto legal.

En el marco de las relaciones de trabajo, la protección de datos personales se ha convertido en parte de la nueva cuestión social, tal como lo ha demostrado la situación de emergencia ocasionada por la pandemia de la Covid-19. Los trabajadores han asumido confiados nuevas formas de trabajo telemático –en algunos casos forzados por mantener sus ingresos– aunque el uso de nuevas tecnologías podría derivar en una muda vulneración de sus derechos.

BIBLIOGRAFÍA

ALEXY, R., *Teoría de los derechos fundamentales,* Ed. Centro de Estudios Políticos y Constitucionales, Madrid, 2014, pag. 67.

ÁLVAREZ CORTÉS, J.C., "La protección de datos de carácter personal en el ámbito de la relación laboral como derecho fundamental inespecífico", Monereo Pérez J.C., y otros (Dir), *Derechos Laborales Fundamentales Inespecíficos*, Editorial Comares, Granada, 2020, p. 315–344.

BAZ RODRÍGUEZ, J., "La ley orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Nº 54, 2019, págs. 49-78.

BAZ RODRÍGUEZ, J., *Privacidad y protección de datos de los trabajadores en el entorno digital*, Ed. Wolters Kluwer, Madrid, 2019.

BAZ TEJEDOR, J.A., "Inteligencia artificial y privacidad del trabajador predictible", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Monográfico Nº 11, 2020.

CERDA SILVA, A., "Intimidad de los trabajadores y Tratamiento de datos personales por los empleadores", *Revista de Derecho Informático*, Nº2, Santiago de Chile, 2003. http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_completo/0,1492,SCID%253D14643%2526ISID%253D292,00.html#

CONTRERAS VÁSQUEZ, P. Y TRIGO KRAMSCSÁK, P., "Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile", *Revista Chilena de Derecho y Tecnología,* Vol. 8 Nº 1, Santiago de Chile, 2019, págs. 69-106.

GOÑI SEIN, J.L., "La protección de las comunicaciones electrónicas del trabajador: la doctrina del Tribunal de Estrasburgo y la jurisprudencia constitucional", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Nº 40, 2018, págs. 12-26.

GOÑI SEIN, J.L., "Uso de los dispositivos digitales en el ámbito laboral", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Monográfico Nº 11, 2020.

JIJENA LEIVA, R., "Actualidad de la Protección de Datos Personales en América Latina. El caso de Chile", Ibarra Sánchez, E. y Téllez Valdes, J. (Cord.), *Memorias del XIV Congreso Iberoamericano de Derecho e Informática*, tomo 1, Universidad Autónoma de Nuevo León, México, 2010. Disponible en: https://biblio.juridicas.unam.mx/bjv/detalle-libro/2940-memorias-del-xiv congreso-iberoamericano-de-derecho-e-informatica-t-1

KUNER, C., "An international legal framework for data protection: Issues and prospects", *Computer Law & Security Review,* Vol. 25, 2009, págs. 307-317. Disponible en https://doi.org/10.1016/j.clsr.2009.05.001

MARTÍNEZ LÓPEZ-SÁEZ, M., "La vigilancia electrónica en el contexto laboral europeo y estadounidense: perfilando el derecho a la protección de datos en el trabajo", *Revista General de Derecho del Trabajo y de la Seguridad Social,* Nº 47, 2017.

MERCADER UGUINA, J., "Nuevos escenarios para el Estatuto de los Trabajadores del siglo XXI: digitalización y cambio tecnológico", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Nº 63, 2020.

MERCADER UGUINA, J., "Protección de datos y relaciones laborales: apuntes prácticos sobre la entrada en vigor del Reglamento (UE) 2016/679", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Nº 41, 2018, págs. 113-126.

MONEREO PÉREZ, J.L. Y FERNÁNDEZ BERNAT, J.A., "Listas negras de trabajadores conflictivos (a propósito de la STS de 12 de noviembre de 2015)", *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, Nº 16, 2016, págs. 83-95.

ORELLANA CANO, A.M., *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores*, Ed. Aranzadi, Pamplona, 2019.

PÉREZ MIRAS, J., *El Derecho a la Protección de Datos y a la Privacidad. Una perspectiva comparada entre la Unión Europea y Estados Unidos,* Tesis Doctoral, Universidad de Sevilla, 2018. Disponible en https://idus.us.es/handle/11441/83475

QUEZADA RODRÍGUEZ, F., "La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile", *Revista Chilena de Derecho y Tecnología,* Vol 1 Nº 1, Santiago de Chile, 2012, págs. 125-147.

SCHERMER, B.W., CUSTERS, B., Y VAN DER HOF, S., "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection*", Ethics and Information Technology*, Nº 16, 2014, págs. 171–182. Disponible en https://doi.org/10.1007/s10676-014-9343-8

SOLOVE, D., "Understanding Privacy", *GWU Legal Studies Research Paper*, Nº 420, 2008. Disponible en https://ssrn.com/abstract=1127888

VILLALBA SÁNCHEZ, A., "El principio de transparencia en la ejecución automatizada del contrato de trabajo: una aproximación jurídica a la tecnología "blockchain" y a la inteligencia artificial", *Nueva Revista Española de Derecho del Trabajo*, Nº 224, 2019, págs. 183-226.

VIOLLIER, P., *El estado de la protección de datos personales en Chile,* Derechos Digitales, Santiago de Chile, 2017. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf